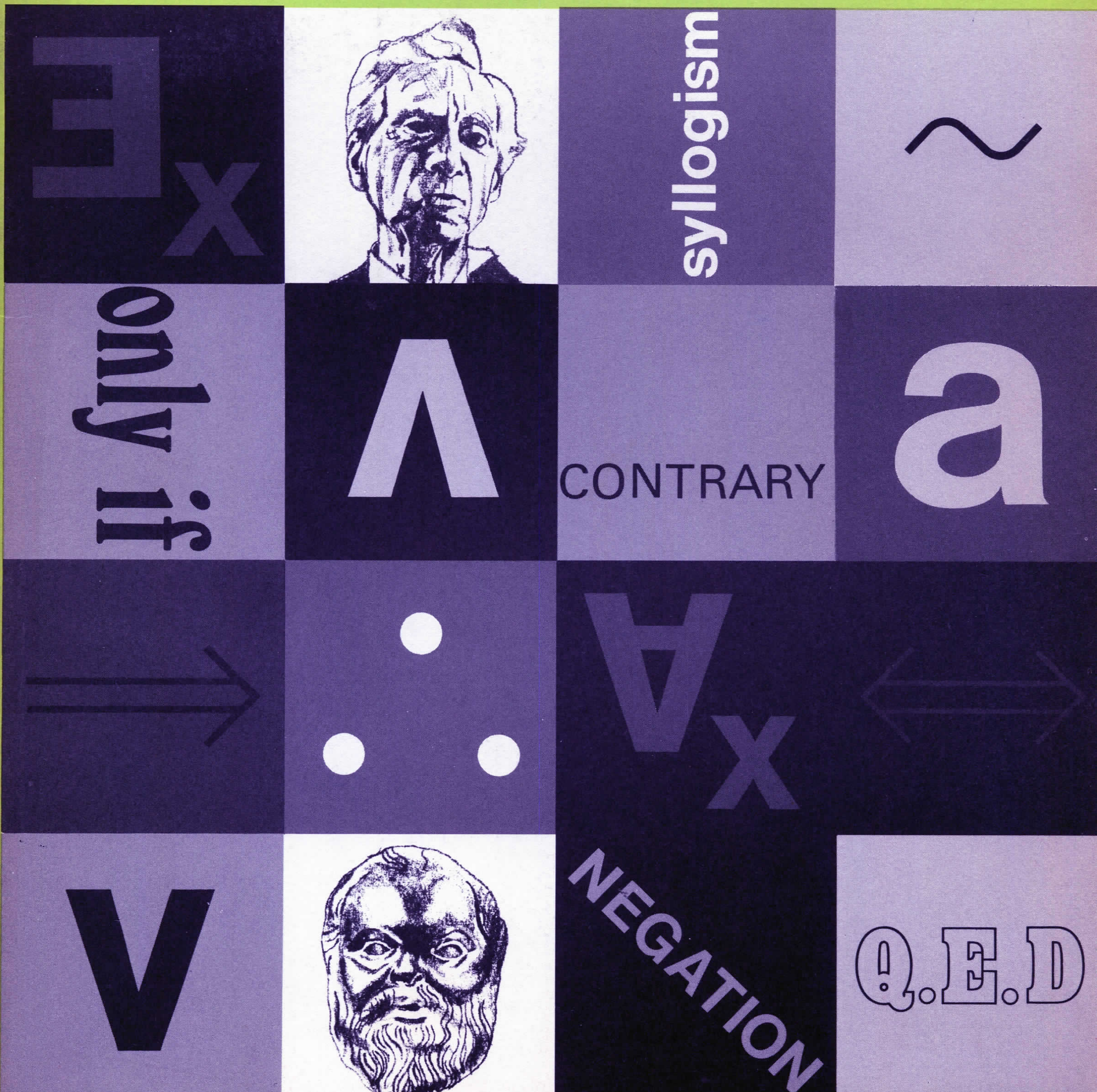
M 100 17

THE OPEN UNIVERSITY

Mathematics Foundation Course Unit 17

Logic II - Proof



The Open University

Mathematics Foundation Course Unit 17

LOGIC II: PROOF

Prepared by the Mathematics Foundation Course Team

Correspondence Text 17

The Open University Press

Professor C. W. Kilmister acted as consultant for this unit.

Open University courses provide a method of study for independent learners through an integrated teaching system including textual material, radio and television programmes and short residential courses. This text is one of a series that make up the correspondence element of the Mathematics Foundation Course.

The Open University's courses represent a new system of university level education. Much of the teaching material is still in a developmental stage. Courses and course materials are, therefore, kept continually under revision. It is intended to issue regular up-dating notes as and when the need arises, and new editions will be brought out when necessary.

Further information on Open University courses may be obtained from The Admissions Office, The Open University, P.O. Box 48, Bletchley, Buckinghamshire.

The Open University Press
Walton Hall, Bletchley, Bucks

First Published 1971

Printed in Great Britain by
J W Arrowsmith Ltd, Bristol 3

Contents

Objectives

The first part of this text is concerned with background material about the history of mathematics and logic, which we think that you will find interesting. It would be inappropriate for us to attempt a formal assessment of your study of this material. Our main objective here is that you should read the text with enjoyment and interest.

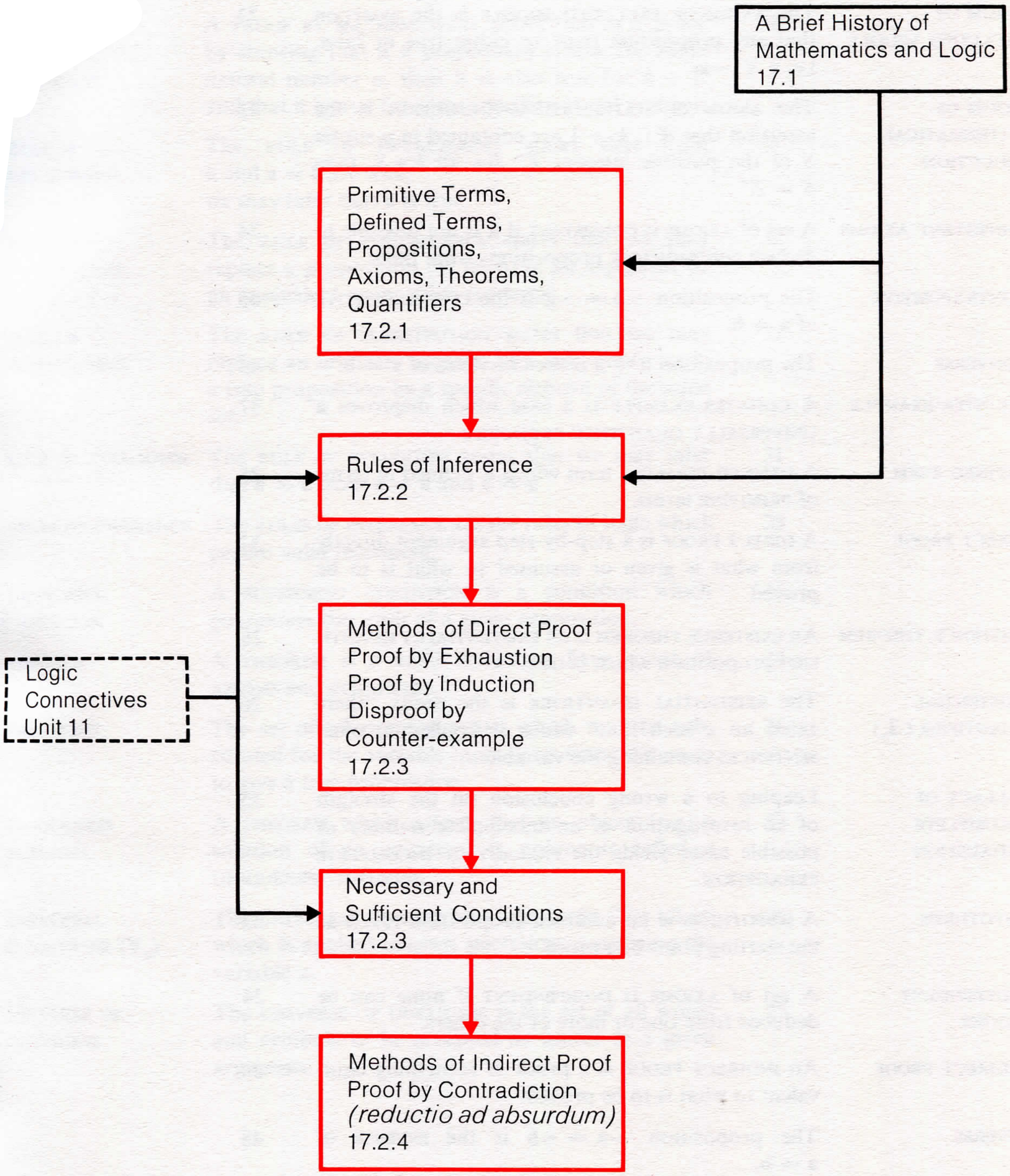
The second part of the text deals with methods of proof used in mathematics. Our main objective here is to enable you to recognize the principal kinds of proof when they arise later in this course or in subsequent courses, and also to set out your own proofs in a consistent logical manner. After working through this second part you should be able to:

(i) write a general essay on mathematical proof;
(ii) define and use correctly the terms listed in the Glossary;
(iii) name the type of proof employed in a given mathematical argument, and state with reasons whether or not the proof is valid;
(iv) construct valid examples of direct and indirect proofs;
(v) define and use correctly the universal and existential quantifiers, $\forall_x$, $\exists_x$.

Note

Before working through this correspondence text, make sure you have read the general introduction to the mathematics course in the Study Guide, as this explains the philosophy underlying the whole course. You should also be familiar with the section which explains how a text is constructed and the meanings attached to the stars and other symbols in the margin, as this will help you to find your way through the text.

Structural Diagram



Glossary

Terms which are defined in this glossary are printed in CAPITALS; these terms appear in section 17.2.

		Page
AXIOM	An AXIOM is a statement about defined objects which is assumed to be true.	24
AXIOM OF EXCLUDED MIDDLE	The AXIOM OF EXCLUDED MIDDLE is the assertion that any proposition must be either true or false, i.e. $\mathbf{a} \vee \sim\mathbf{a}$.	24
AXIOM OF MATHEMATICAL INDUCTION	The AXIOM OF MATHEMATICAL INDUCTION is the assertion that if 1, $k + 1$ are contained in a subset S of the positive integers Z^+ for all $k \in S$, then $S = Z^+$.	41
CONSISTENT AXIOMS	A set of AXIOMS is CONSISTENT if it is not possible to deduce contradictory propositions from them.	24
CONTRAPOSITIVE	The proposition $\sim\mathbf{b} \Rightarrow \sim\mathbf{a}$ is the CONTRAPOSITIVE of $\mathbf{a} \Rightarrow \mathbf{b}$.	46
CONVERSE	The proposition $\mathbf{b} \Rightarrow \mathbf{a}$ is the CONVERSE of $\mathbf{a} \Rightarrow \mathbf{b}$.	43
COUNTER-EXAMPLE	A COUNTER-EXAMPLE is a case which disproves a UNIVERSALLY QUANTIFIED conjecture.	37
DEFINED TERM	A DEFINED TERM is a term which is defined in terms of PRIMITIVE terms.	25
DIRECT PROOF	A DIRECT PROOF is a step-by-step argument directly from what is given or assumed to what is to be proved.	34
EXISTENCE THEOREM	An EXISTENCE THEOREM is an EXISTENTIALLY QUANTIFIED proposition which is true.	28
EXISTENTIAL QUANTIFIER ($\exists_x$)	The EXISTENTIAL QUANTIFIER is the prefix "there exists an x such that" which is applied to OPEN SENTENCES containing the variable x.	26
FALLACY OF INCOMPLETE EXHAUSTION	Leaping to a wrong conclusion on the strength of an investigation of an incomplete number of possible cases yields the FALLACY OF INCOMPLETE EXHAUSTION.	35
HYPOTHESIS	A HYPOTHESIS is an assumed proposition taken as the starting point of a proof.	33
INDEPENDENT AXIOMS	A set of AXIOMS is INDEPENDENT if none can be deduced from one or more of the others.	24
INDIRECT PROOF	An INDIRECT PROOF is a proof of something equivalent to what is to be proved.	34
INVERSE	The proposition $\sim\mathbf{a} \Rightarrow \sim\mathbf{b}$ is the INVERSE of $\mathbf{a} \Rightarrow \mathbf{b}$.	48
NECESSARY CONDITION	A NECESSARY CONDITION is a condition which must hold for a given proposition to be true, but which does not guarantee the truth of the proposition.	46
OPEN SENTENCE	An OPEN SENTENCE is a sentence containing a variable, which becomes a proposition only when the variable is replaced by a DEFINED TERM.	25
PRIMITIVE TERM	A PRIMITIVE TERM is a term, the meaning of which is presumed without formal definition.	23

		Page
PROOF BY CONTRADICTION (*reductio ad absurdum*)	A PROOF BY CONTRADICTION is a proof that a proposition, contradictory to what we want to prove, is false.	51
PROOF BY EXHAUSTION	A PROOF BY EXHAUSTION is a proof by examining every possible case.	35
PROOF BY MATHEMATICAL INDUCTION	A PROOF BY MATHEMATICAL INDUCTION is a proof by showing that if a proposition is true for some natural number n, then it is also true for $n + 1$, and that it is true for some specific natural number.	38
RULE OF DETACHMENT	The RULE OF DETACHMENT states that from $\mathbf{a}$ and $\mathbf{a} \Rightarrow \mathbf{b}$ are true, we may infer that $\mathbf{b}$ is true.	31
RULE OF EQUIVALENCE	The RULE OF EQUIVALENCE states that we may replace a proposition (or term) in an argument by an equivalent proposition (or term).	32
RULE OF SUBSTITUTION	The RULE OF SUBSTITUTION states that we may replace an arbitrary element of a non-empty set in a true proposition by a specific element of the same set.	32
RULE OF SYLLOGISM	The RULE OF SYLLOGISM states that we may infer that $\mathbf{a} \Rightarrow \mathbf{c}$ from $\mathbf{a} \Rightarrow \mathbf{b}$ and $\mathbf{b} \Rightarrow \mathbf{c}$.	31
RULES OF INFERENCE	The RULES OF INFERENCE are the rules of logic which permit valid reasoning.	25
SUFFICIENT CONDITION	A SUFFICIENT CONDITION is a condition which guarantees the truth of a given proposition.	46
THEOREM	A THEOREM is a valid deduction from a set of AXIOMS and definitions.	24
TRUTH SET	The set of all DEFINED TERMS which may be substituted for the variable in an OPEN SENTENCE so as to give a true proposition.	26
UNIQUENESS THEOREM	A THEOREM which asserts that an object (e.g. a solution of an equation) is unique is called a UNIQUENESS THEOREM.	53
UNIVERSAL QUANTIFIER ($\forall_x$)	The UNIVERSAL QUANTIFIER is the prefix "for all x" which is applied to OPEN SENTENCES containing the variable x.	26
UNIVERSE OF DISCOURSE	The UNIVERSE OF DISCOURSE is the set of all words and symbols to be accepted as usable in a given argument.	25

Notation

The symbols are presented in the order in which they appear in the text.

		Page
$\Rightarrow$	The symbol of implication (read as "implies" or "if . . . , then . . .").	4
$\cap$, $\cup$	Binary operations in a Boolean algebra.	15
$\longleftrightarrow$	"corresponds to".	17
$\sim$	The symbol of negation (read as "not").	18
$\varnothing$	The empty set.	18
$\wedge$	The symbol of conjunction (read as "and").	18
$\mathbf{a}$	The proposition **a**.	20
$\vee$	The symbol of alternation (read as "or").	20
$B\hat{L}D$	The angle $B\hat{L}D$.	20
$\exists_x$	The existential quantifier (read as "there exists an x such that" or "for *some* x").	26
$\forall_x$	The universal quantifier (read as "for *all* x").	27
$A \subset B$	Set A is a proper subset of set B.	27
$\circ$	The symbol for a binary operation.	33
$\mathbf{a}_x$	An open sentence including the variable x.	37
Z^-	The set of negative integers.	38
D	The differentiation operator.	39
D^n	$\underbrace{D \circ D \circ \cdots \circ D.}_{n \text{ terms}}$	39
$\Leftrightarrow$	The symbol of equivalence (read as "if and only if").	47

Bibliography

C. B. Allendoerfer and C. O. Oakley, *Principles of Mathematics*, 2nd ed. (McGraw-Hill, 1963).

Chapter 1 discusses the nature of mathematics, introduces the relation between logic and set theory, and considers a number of methods of proof. The first part of Chapter 3 is devoted to mathematical induction.

C. W. Kilmister, *Language, Logic and Mathematics* (English Universities Press, 1967).

This book provides a brief sketch of Greek logic and its algebraic representation by Boole, and is then devoted to discussing the main problems in logic stimulated by Cantor's set theory, *Principia Mathematica*, Hilbert and Gödel.

H. De Long, *A Profile of Mathematical Logic* (Addison-Wesley, 1970).

This book gives a fairly full history of mathematics and logic, and discussion of axiomatic theory, metalogic and the philosophical implications of mathematical logic. It is detailed but very readable, and is rich in quotations and examples.

M. L. Bittinger, *Logic and Proof* (Addison-Wesley, 1970).

This is a paperback consisting almost entirely of definitions, exercises and answers.

List of Names of Mathematicians and Logicians Referred to in the Text

Abelard, Peter	(1079–1142)
Aristotle of Stagira	(384–322 B.C.)
Bacon, Roger	(*c.* 1214–1292)
Boole, George	(1815–1864)
Brouwer, L. E. J.	(1881–1968)
Cantor, Georg	(1845–1918)
Cauchy, Augustin Louis	(1789–1857)
De Morgan, Augustus	(1806–1871)
Dodgson, Charles (Lewis Carroll)	(1832–1898)
Eubulides	(4th century B.C.)
Euclid	(4th–3rd centuries B.C.)
Eukleides	(*c.* 430–*c.* 360 B.C.)
Euler, Leonhard	(1707–1783)
Fermat, Pierre	(1601–1665)
Frege, Gottlob	(1848–1925)
Gödel, Kurt	(1906–)
Hilbert, David	(1862–1943)
Kronecker, Leopold	(1823–1891)
Leibniz, Gottfried Wilhelm	(1646–1716)
Lobachevski, Nikolai	(1793–1856)
Lull, Raimon	(*c.* 1235–1315)
Peano, Guiseppe	(1858–1932)
Plato	(*c.* 428–*c.* 348 B.C.)
Pythagoras	(*c.* 566–*c.* 497 B.C.)
Riemann, Bernhard	(1826–1866)
Russell, Bertrand	(1872–1970)
Schröder, Ernst	(1841–1902)
Venn, John	(1834–1923)
Whitehead, Alfred North	(1861–1947)
Zeno	(495–435 B.C.)

17.0 INTRODUCTION

17.0

Introduction

We took our first look at logic in *Unit 11*, and you may have been a little surprised that nowhere in that unit did we study *proof* as such. However, we shall now make good this seeming deficiency, as the subtitle of this unit indicates.

In *Unit 11* we studied propositions and the logical connectives by means of which they can be combined, and we saw how an algebra of propositions could be constructed which was essentially the same as the algebra of sets, and which could be realized physically by switching networks. In constructing such an algebra, we were indeed establishing a link between logic and mathematics, but we did not examine what is perhaps the most obvious link between these two disciplines, namely the ways in which mathematicians use logic to develop mathematical arguments by proving theorems.

In this text, we shall concentrate upon the idea of *proof*. We shall devote the first part of the text to looking at its historical development from ancient times to the present day, and the second part to an examination of the most common types of proof used in mathematics.

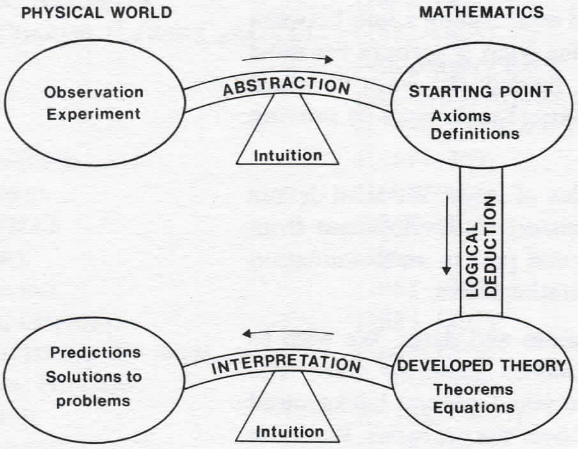
In section 17.1 we mention quite a lot of names and dates. We wish to emphasize that *you are not expected to memorize names or dates.* The historical part of this text is intended to give you a general background to the development of mathematics and logic over the centuries. We think that such a historical survey is valuable, and we hope that you will find it interesting and stimulating. If, however, you are very short of time, then you will not prejudice your studies by regarding section 17.1 as a "purely cultural option" which you can safely put on one side to be read at leisure when pressures upon your time have decreased.

The second part of the text is, however, intended for careful and immediate study. In the earlier units, we have not troubled you unduly with formal mathematical proofs, though we have used words such as *proof*, *definition*, *property*, etc., on the assumption that these were sufficiently generally understood for you not to be worried by our use of them. As the course progresses, we shall present rather more proofs than we have done up to now; so this is an appropriate stage to discuss the kinds of proof commonly used in the development of a mathematical argument. No study of mathematics can avoid proof. Intuition can start us off, but sooner or later it becomes essential that we check to see whether or not we have built on secure footings. We must be prepared to put all that we have done to the test, and it is logic that enables us to do this.

The starting point for every science is the world around us. We observe nature; we experiment and observe the results of our experimentation. Mathematics is in a similar situation, although it is dealing fundamentally with abstractions. The mathematician has to begin somewhere, and he usually chooses to begin with abstractions which to some extent correspond to things which are observed in nature. Of course, he is not compelled to do this; he can begin with a list of symbols and some arbitrary rules for manipulating them, but unless, at some point, there is some reference either to the real world or to some other mathematics having its roots in natural phenomena, his labours may well be thought to be little more than an intellectual game.

In the choice of a starting point, intuition plays a significant role, often suggesting not only the kind of abstraction which is meaningful, but also the direction in which the mathematics should be developed if it is to prove fruitful. Again, in pointing the way to possible areas of application of a developed mathematical theory, intuition is of great importance.

So we can think of intuition as a major support for the bridge between the physical world and the abstract world of mathematics, which has to be crossed in both directions: first, when a mathematician is abstracting from nature the axioms and definitions which are to form his starting point, and is looking for a possible path to explore, and later, after a journey of logical development, when he wishes to match his developed mathematical theory against the problems of his environment. We can illustrate this in the following way:



You will notice that we have introduced the word *deduction* into the diagram above. This is because we want to make it clear that when we are considering *proof* we are, in fact, considering the end-product of a *deductive* process. You may have encountered the phrase *inductive proof*, but there is a sense in which this is self-contradictory. So-called *inductive proof* (not to be confused with *proof by mathematical induction*) is the process of coming to a *probable conclusion* on the basis of a large number of occurrences of some event. It may have its part to play in the experimental sciences where events, both natural and experimental, are observed, and an attempt is made to formulate "laws" which are consistent with observation and by means of which future events may be predicted successfully. Such a process *does not constitute proof*, and we shall not be concerned at all in this text with inductive logic, since this plays only a very small part in mathematics as an occasional pointer to a possible truth. As has been said elsewhere, "accumulation of examples is no more mathematics than a dictionary is a novel!"

Before starting on our history of logic, we mention briefly the question of "proof and truth". It is a popular misconception that we can arrive via purely logical processes at that which we can regard as *true*. No answer was given to Pontius Pilate, the Roman Governor of Judaea, when he asked the profound question, "What is truth?", and it is doubtful if an acceptable answer can ever be given with complete certainty. So logic does not attempt to answer such questions as "Is this given statement *true?*" but only such questions as "Is this deduction from given statements *valid?*" — an altogether different question. The *truth* of a deduction depends not only upon the process of logical reasoning but also upon the truth of the initial statements. In the last resort, there must always be some statements which we accept without proof as intuitively obvious (or as an "act of faith").

Some philosophers have attempted to formalize this distinction between *truth* and *validity* by speaking of the *matter* and the *form* of an argument. Truth is said to depend upon the *matter* and validity upon the *form* only.

But this does not really help us to arrive at a satisfactory definition of what is *true*, since we are merely thrown back upon the requirement for a satisfactory definition of *matter*. So we shall continue to confine our use of the word *true* to that which we adopted in *Unit 11*, that is, as one of two possible truth values of a proposition, and in this text we shall concentrate upon *proof* in terms of *validity of deductive reasoning*, leaving the more profound question to those who have the time to search for the undiscoverable.

17.1 HISTORICAL SURVEY OF LOGIC

17.1

OPTIONAL MATERIAL

Optional Material
*

17.1.0 Introduction

17.1.0

The history of logic is to a great extent the history of the interaction of logic and mathematics, since the stimulus for each major development in logic seems to have come largely from developments in mathematics. This is not meant to suggest that philosophy and theology have played no part in the development of logic through the centuries, but, if anything, their influence has tended to be conservative rather than progressive, and so, particularly in a Mathematics Foundation Course, we make no apology for concentrating our history upon those areas where the two disciplines of logic and mathematics have interacted and stimulated each other, since this makes a fascinating and fairly complete story in its own right.

We divide our history into two main sections, which we shall call *ancient logic* and *modern logic*. There is indeed an intermediate period, covering several centuries and usually known as the *scholastic period*, which we shall mention briefly, but it is essentially a period during which ancient logic remained virtually unchanged, though here and there aspects of it were challenged or directed into an unusual channel by a particularly venturesome mind.

17.1.1 Ancient Logic

17.1.1

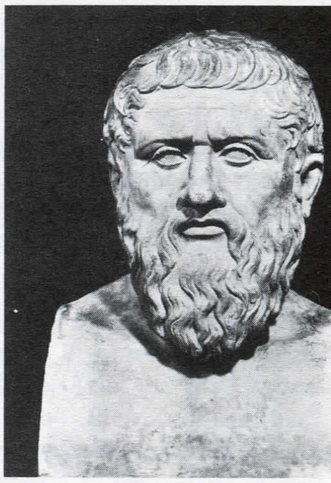
ARISTOTLE OF STAGIRA, 384–322 B.C., is generally accepted as the man who created the study of logic, and indeed, in one of his writings he seems to make this very claim for himself.

Aristotle

Aristotle's study was, however, foreshadowed in that the works of many ancient writers before him, especially PLATO, *c.* 428–*c.* 348 B.C., contain numerous arguments which are set out in a logical manner, and clearly show that many of the processes of logical reasoning were well known long before his day. Some of these arguments must have been used in the study of geometry, which had been considered important from very early times. It is reputed that over the entrance of Plato's Academy there was inscribed in Greek:

Let no one ignorant of geometry enter my door.

Aristotle's claim to be the creator of logic rests upon his being the first to codify formally the existing rules of logic. In fact, Aristotle codified the *theory of syllogism*, which we now know to be only a small part of logic, though many philosophers have been so fascinated by it that they have been misled into assuming that it is the greater part (or even the whole) of logic.

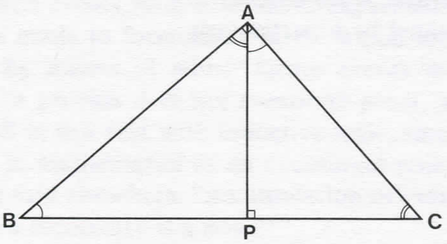


Plato

An important motivation for the study of logic probably came from the desire to overcome paradoxes. A great number of paradoxes had been discovered. Some of these were difficulties arising out of the use (or misuse) of language. Some were related to difficulties of a more mathematical kind, and we shall look briefly at two of these.

Virtually every child at some time or other during his schooldays comes across the theorem which bears the name of Pythagoras, namely the theorem that the sum of the squares of the shorter sides of a right-angled triangle is equal to the square of the hypotenuse. PYTHAGORAS, *c.* 566–*c.* 497 B.C. may or may not have been the first to formulate this theorem, but it is thought that he may originally have proved it using similar triangles.

Pythagoras



ABC is a triangle, right-angled at *A*, and *AP* is the perpendicular from *A* to *BC*. From the angles shown equal in the figure, it follows that the triangles *ABC*, *PBA* and *PAC* are all similar triangles, and, in particular,

$$\frac{AC}{CP} = \frac{BC}{AC} \Rightarrow AC^2 = BC \cdot CP$$

and

$$\frac{AB}{BP} = \frac{BC}{AB} \Rightarrow AB^2 = BC \cdot BP.$$

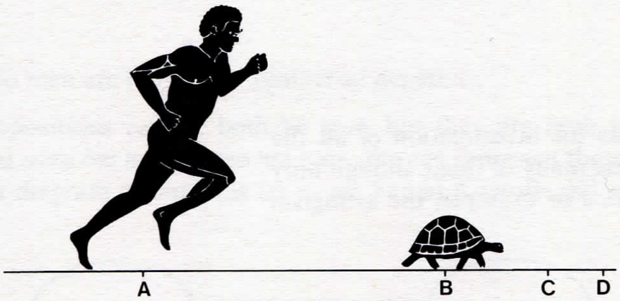
Addition now gives

$$\begin{aligned} AB^2 + AC^2 &= BC(BP + CP) \\ &= BC^2. \end{aligned}$$

This all seems very sound. The trouble was that the theorems about similar triangles had in their turn been proved by dividing off sides into parts so that m parts of one side were equal to n parts of the other, an underlying assumption being that *any length was expressible in terms of the ratio of two integers.*

The discovery that the diagonal of a unit square could not be so expressed was a paradox which threw the whole Pythagorean school into confusion, since it undermined not only their accepted proofs of geometrical theorems, but also their whole belief in *number* as the unifying principle of arithmetic and geometry. So stunned were they by this paradox and so fearful that it should become public, that it is said that they were sworn never to reveal it.

Another paradox which arose concerns the swift runner, Achilles, and the tortoise. The argument goes something like this. If Achilles starts at point A, some fixed distance behind the tortoise at point B, and they both travel along a path at their respective maximum speeds, by the time Achilles reaches B the tortoise will have moved to C. Then, by the time Achilles reaches C the tortoise will have moved to D. In each case the tortoise's lead is reduced, but the argument can be continued for ever over smaller and smaller distances. So Achilles never catches up with the tortoise . . . an obviously false conclusion!



Other paradoxes arose out of the Greek concept of infinity, but detailed evidence of much of this is scanty. It was clear, however, that the embarrassment of such paradoxes indicated a need for the clarification of the nature of argument and a re-examination of the assumptions upon which existing arguments were based. Aristotle's *theory of syllogism* provided a basis for argument which was to last for twenty centuries with only comparatively minor modifications, though it was unable to resolve many of the paradoxes which were known in his day.

The basis of the theory is the assumption that all correct argument can be analysed into sentences of one particular form, which we call the *subject-predicate proposition.* Examples are:

All men are mortal.
No fish is a bird.
Some Greeks are wicked.
Some women are not mothers.

In each case there is a *subject* of the sentence, which is *quantified* so as to specify either *all* members of a class or merely *some* members of a class, joined by a verb to a *predicate.* If subject and predicate are denoted by S, P respectively, then we have the possibilities:

all S is P;
no S is P;
some S is P;
some S is not P.

These correspond to our four examples, and are termed respectively:

universal affirmative;
universal negative;
particular affirmative;
particular negative.

An *argument*, for Aristotle, was a collection of such propositions related in a certain way, and further, Aristotle assumed that a valid argument could be broken down into a succession of basic arguments each composed of only three propositions and known as *syllogisms*. In a syllogism, two of the propositions form the *premisses* and the third the *conclusion*.

We shall examine a typical syllogism:

If all men are mortal
and all Greeks are men,
then all Greeks are mortal.

Using S, P for the subject and predicate of the conclusion "all Greeks are mortal", we note that the first premiss includes P and the second includes S. P and S were known respectively as the *major* and *minor* terms, and so the premiss including P was called the *major premiss* and that including S the *minor premiss*. The term "men" appears in each premiss but not in the conclusion, and was known as the *middle term*, which we shall denote by M. The argument is thus:

If all M is P
and all S is M,
then all S is P.

The principal achievement of Aristotle was his investigation of all the possible forms of syllogism; there are a great many of them, though only a proportion give rise to a valid argument. For example, the syllogism we have just been discussing has the form:

MP
SM
SP.

First, S and P can occur in their respective premisses either as subject or predicate, the middle term being the corresponding other part of the premiss. (Remember that S and P are respectively the subject and predicate *of the conclusion*.) This gives four combinations known as the four *figures* of the syllogism:

I	II	III	IV	Figure
MP	PM	MP	PM	(major premiss)
SM	SM	MS	MS	(minor premiss)
SP	SP	SP	SP	(conclusion)

In each figure, the propositions can be either universal or particular, affirmative or negative. There are thus $256 (= 4 \times 4 \times 4 \times 4)$ possible syllogisms, though many of these are invalid arguments in which the conclusion does not follow from the premisses. An example of such an invalid syllogism in figure I is:

If no M is P
and all S is M,
then some S is P.

Because the Aristotelian syllogism has little relevance to mathematical reasoning, we shall not pursue this topic here, but it is important to remember that the classification of all valid forms of syllogism was a substantial task justifying in no small measure Aristotle's claim to be the founder of the study of logic.

Before leaving the work of Aristotle, we should mention the so-called *square of opposition*, since this does have some relevance to proof in mathematics. Given the four types of proposition:

universal affirmative	(all S is P);
universal negative	(no S is P);
particular affirmative	(some S is P);
particular negative	(some S is not P),

and *keeping the same S and P throughout*, it is clear that these stand in particular relationships to each other. What can be said about these relationships?

Two propositions are *contradictories* if when either is true the other must be false, and vice versa. Consider, for example, the propositions:

All men are liars	(universal affirmative)
Some men are not liars	(particular negative).

If the former is true, the latter must be false, and conversely. Also, if the former is false, the latter must be true, and conversely. They are thus *contradictory propositions.*

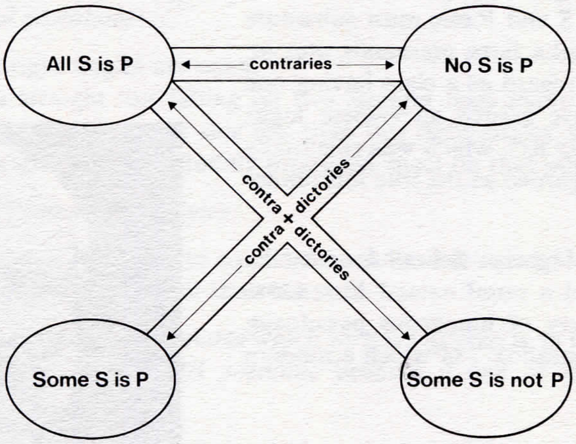
Two propositions are *contraries* if they cannot both be true, but both may be false. Thus the *contrary proposition* to

All men are liars (universal affirmative)

is

No men are liars (universal negative).

These propositions cannot both be true, but they are both false if we accept that *some but not all* men are liars. We can represent these relationships by a diagram, though (as far as we know) Aristotle did not do so:



The remaining sides of the "square" express the relationship between:

All S is P	and	Some S is P;
No S is P	and	Some S is not P;
Some S is P	and	Some S is not P.

Aristotle assumed that in the first two cases the second proposition (the lower on the diagram) can be deduced from the first, and later logicians gave the name *subalternation* to this relationship. This assumption may, however, be challenged on the grounds that the "set of all S" may be empty. Aristotle also indicated that he was aware of a relationship between

Some S is P and Some S is not P,

later to be known as *sub-contraries.*

We ask a further question here: "When is it generally permissible to interchange *S* and *P* in a proposition?" The *converse* of a proposition of the form *SP* is the identical proposition with *P* and *S* interchanged, and this exchange is, in general, permissible only in a proposition which is either of the form:

No *S* is *P* (universal negative)

or of the form:

Some *S* is *P* (particular affirmative).

For example, if it is true that

no birds are mammals,

then it is also true that

no mammals are birds.

Also, if

some Greeks are liars,

then

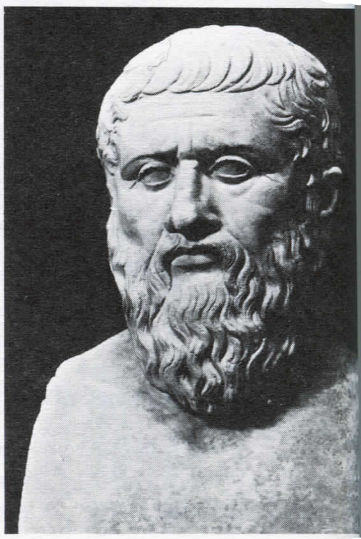
some liars are Greeks.

However, in the case of the universal affirmative, for example,

all men are animals,

we may not exchange *men* and *animals* and retain a true proposition, and similarly in the case of the particular negative. This is not to say that we may never exchange *S* and *P* in a universal affirmative—consider, for example, "all *S* is *S*"—but we may not automatically do so, as we may in the case of a universal negative or a particular affirmative.

It is important to note that Aristotle's theory of syllogism is essentially a *logic of classes* in that for the "variables" *S* and *P* one must substitute classes of objects such as all men, some Greeks, liars, mammals, etc., or, occasionally, a single object (which we can regard as a class having one member). There is, however, known to have existed an ancient logic, that of the Stoics, founded by ZENO, 495–435 B.C., which was essentially a *logic of propositions* and as such can be regarded as the true forerunner of the logic of today.


Zeno

Stoic logic evolved from the logic of the Megarian School founded by EUKLEIDES, *c.* 430–*c.* 360 B.C. Eukleides had a pupil named EUBULIDES whose fame rests largely upon his discovery of numerous paradoxes, the most notable being the so-called "liar paradox", of which a modern form is:

This sentence is untrue.

Suppose that the sentence is *true*, then it becomes true that it is untrue. Similarly, suppose that the sentence is *false*, then it follows that it is true. (This paradox became very famous indeed and is even mentioned by St. Paul in his first letter to Titus.) The "liar paradox" arises out of the fact that the sentence *refers to itself* in a special way. It is only in recent years that the distinction between a *language* and a *metalanguage* in which one discusses a language has been clarified.

Of course, in many cases of self-reference no paradox arises. There is, for example, no problem associated with the English sentence:

This proposition consists of exactly seven words,

but we might well ask what would happen if it were translated into Chinese.

Unfortunately only fragments remain of the Megarian–Stoic writings, and so ancient logic has come to mean very largely the syllogistic logic of Aristotle. Neither the logic of Aristotle nor that of the Megarian–Stoic logicians was able to unravel the kinds of paradox which we have mentioned.

Eukleides, who is mentioned more than once in the writings of Plato, is not to be confused with the author of the *Elements*, the Greek mathematician EUCLID, who founded a school at Alexandria sometime around 300 B.C. (Some of the medieval philosophers did confuse the two.) The *Elements* runs to thirteen volumes, of which nine deal with plane and solid geometry and four with arithmetic. Much of the material is a systematic arrangement of previously known mathematics and is, in fact, the work of more than one man. (It has even been suggested that the name Euclid was deliberately used by several writers, rather as the name Bourbaki has been used in modern times.)

Euclid

It is not clear exactly what purpose Euclid had in mind in writing the *Elements*, but the monumental result has been described as the "greatest textbook of all times". Indeed, it was still in regular use in schools in the present century, a survival of well over 2000 years. The work begins with a series of 23 *definitions*, 5 *postulates* and 5 *common principles*, and from these a very large number of *theorems* are deduced. This provides a very early example of what we call the *axiomatic method*, which is closely related to modern developments of mathematical logic. We shall not list all the definitions, etc., here, but give one or two examples, including that of the *parallel postulate* to which we shall refer later.

Examples of *definitions*:

> A point is that which has no part.
> A line is a breadthless length.
> A surface is that which has length and breadth only.

Examples of *postulates*:

> All right-angles are equal.
> If a straight line falling on two straight lines make the interior angles on the same side less than two right-angles, then the two straight lines, indefinitely produced, meet on that same side.

Examples of *common principles*:

> If equals be added to equals, the wholes are equal.
> The whole is greater than the part.

The second of the two postulates which we have quoted is, in fact, Euclid's fifth, known as the *parallel postulate* because it can be shown to be equivalent to:

> Through a given point outside a given straight line only one line can be drawn parallel to that straight line.

Both this postulate, and the common principle that "the whole is greater than the part", were accepted as *true* until developments (which we shall mention later) in the nineteenth century produced geometric structures in which they did not hold.

We can now summarize what we have called *ancient logic* under three main headings:

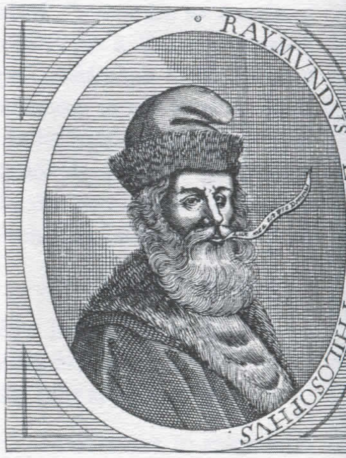
(1) Aristotle's theory of syllogism;
(2) Megarian–Stoic logic;
(3) Euclid's *Elements*.

(1) provides an extensive theory of argument based on the syllogism, which was the major influence on philosophy and theology for twenty

centuries. (2) provides a first attempt at the analysis of paradoxes, but comparatively little survives of the material. (3) provides an extensive and systematic presentation in axiomatic form of most of what was known in ancient times of geometry and arithmetic.

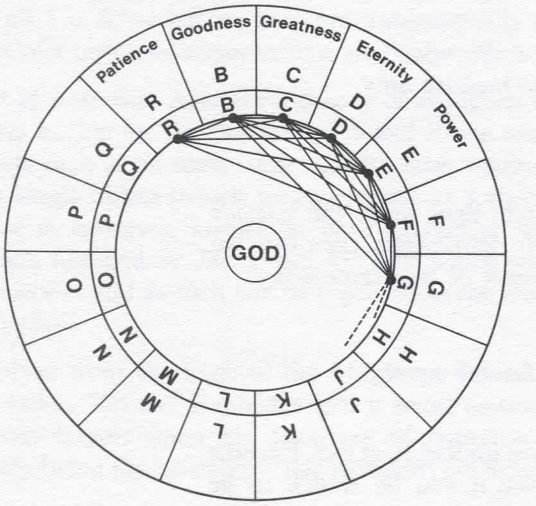
Following the ancient period, there were many centuries when the development of logic and mathematics was virtually at a standstill. There are a few names, however, deserving of mention, in the period which bridges the gap between ancient and modern logic. This period is usually known as the *scholastic period*, commencing with the work of PETER ABELARD, 1079–1142. Although popularly well-known for his romantic affair with his pupil Heloise, his significant contribution to logic was his application of this study to the theology of the day. It was this, rather than his love-life, that was the root cause of his conflict with ecclesiastical authority.

Peter Abelard



Raimon Lull

RAIMON LULL, *c.* 1235–1315, was a Catalan mystic born in Majorca who, after a youth spent in wild living, turned to religion and philosophy. Aristotle's work had (as far as we know) contained no diagrams, though these were liberally added by subsequent commentators and much elaborated during the scholastic period. Lull made the first serious attempt to employ geometrical figures for the purpose of discovering logical truths. In his *Ars Magna*, he frequently uses the idea of concentric rotating circles in order to obtain complete sets of combinations of concepts such as *goodness*, *greatness*, *eternity*, and so on. In the centre of the concentric circles appears the main object whose attributes are being investigated, *God*, *the soul*, *virtue*, etc. We give just one example:



God appears here as the object under discussion. There are two rotating circles, centred on *God*, and containing 16 compartments labelled with letters standing for divine properties, for example, *R* for *patience*, *B* for *goodness*, etc. Either by rotating the circles, or by drawing connecting lines (some of which we have shown) we arrive at 120 different combinations of two letters which are supposed to tell us something additional about God. Thus the combination *BD* tells us that "His goodness is eternal", and the combination *CE* that "His greatness is powerful", etc.

Lull designed many such figures, some quite simple, some very complicated and involving no less than 13 concentric circles. By these figures he believed that one could discover all the necessary combinations of terms out of which arguments could be constructed, and at least one of the figures was explicitly devoted to logic itself, the compartments standing for such concepts as *affirmation*, *negation*, *doubt*, *similarity*, *contrariety*, etc.

Many of the figures were vividly coloured, and were popularly believed to have magical properties. Naive and trivial as all this may seem today, it was a very real attempt to use geometric ideas to clarify logical argument and, as such, may be thought of as a first step towards the Venn diagrams (set diagrams) which are familiar to us today.

A contemporary of Lull was the English philosopher and scientist, ROGER BACON, *c.* 1214–1292. He was associated with the philosophical schools of Oxford and Paris, where he lectured extensively on Aristotle. He was one of the most original thinkers of the scholastic period of logic, but was condemned and for a time imprisoned by the Church authorities. Whilst his contributions to thought were not specifically mathematical, he produced his *Opus Maius*, a compendium of all branches of knowledge, and he foresaw the magnifying properties of convex lenses, the possibility of mechanically propelled boats and flying machines, as well as the extensive use of gunpowder.

Roger Bacon

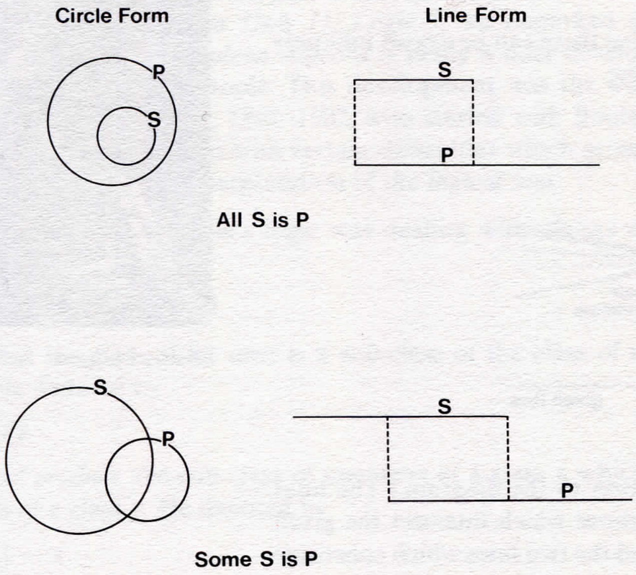
17.1.2 Modern Logic

17.1.2

Modern logic is usually considered to begin with the work on the algebra of logic by GEORGE BOOLE, 1815–1864, but we shall take up our history again over a century earlier with the German philosopher and mathematician GOTTFRIED WILHELM LEIBNIZ, 1646–1716.

Leibniz was probably the first mathematician to take up the idea of logic in earnest. This remarkable man is best known for his pioneering work in the differential and integral calculus, and was the first proposer of a universal symbolic language. He anticipated Boole in early attempts to symbolize logical arguments in algebraic terms, though his efforts here had little or no influence as they were not published until 1903. He was also interested in geometrical representation of syllogisms, and was the first to use what we know as Venn diagrams (200 years before Venn). As well as circle (set) diagrams, he used diagrams with lines, as he considered the latter easier to work with. Two examples will give you the general idea.

George Boole

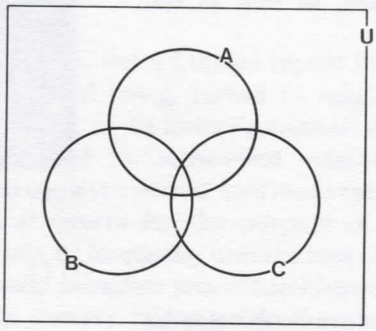


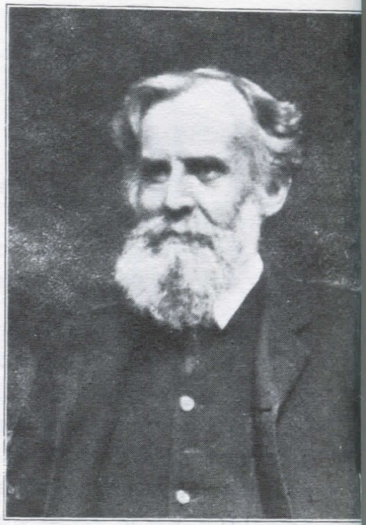
Gottfried Wilhelm Leibniz

The circle diagrams became really popular at the time of the Swiss mathematician, LEONHARD EULER, 1707–1783, with whose name they are sometimes associated, but it was JOHN VENN, 1834–1923, who collected together the different diagrams in general use and who, with the benefit of Boole's work as reference, introduced the three circles drawn so as to overlap in all possible ways, thus dividing the plane into 8 regions. The last contributor to this story of circle diagrams was CHARLES DODGSON, 1832–1898 (LEWIS CARROLL of *Alice in Wonderland* fame), who enclosed Venn's circles in an outer rectangle (or square) representing the *universe of discourse*, thus giving us the Venn diagram in the form in which we use it today.

Leonhard Euler

Venn Diagram for 3 sets





John Venn

(Note that the word "circle" in the above discussion is not meant literally; the geometrical representation of the sets does not have to be a circle, as such.)

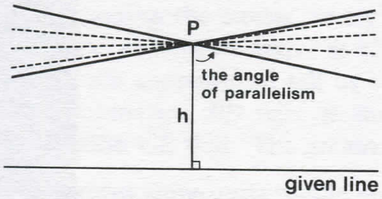
We have referred earlier (page 9) to Euclid's *parallel postulate.* For many centuries numerous attempts were made to *prove* the postulate (or an equivalent one) using the remaining definitions, postulates, and common principles, but without success. It was, however, always regarded as a self-evident truth until the Russian mathematician, NIKOLAI LOBACHEVSKI, 1793–1856, discovered and published details of a *non-Euclidean geometry* obtained by modifying the postulate. In fact, it is probable that there were several almost simultaneous discoveries of non-Euclidean geometries, but the topic is usually associated with Lobachevski, since he was the first to publish his results.

Charles Dodgson

In Lobachevskian geometry, Euclid's parallel postulate is replaced by the following:

> Through a point outside a given line there can be drawn infinitely many lines parallel to the given line.

Consider the following diagram:



(Beware of giving a Euclidean interpretation to the diagram.) The lines through *P* are divided into two classes: those which intersect the given line, and those which do not intersect it, and the two lines which constitute the boundary between the classes make an acute angle with the perpendicular (as shown), known as the *angle of parallelism*, the exact value of which depends upon the height h of the point P above the given line. As h increases, the angle tends to 0: as h decreases, the angle tends to 90°.

The interesting feature of Lobachevskian geometry is that it gives an *absolute measure of distance*, that is to say, one that does not depend upon the choice of unit (e.g. metre, yard). This is because the distance (height) h is measured entirely in terms of angle, a dimensionless quantity (see *Unit 3, Operations and Morphisms*, section 3.2.4). Another consequence of Lobachevski's postulate is that the sum of the interior angles of a triangle is less than 2 right-angles, but tends to the Euclidean value as the area of a triangle tends to zero. Since in this geometry distance depends only on *angles*, equiangular triangles necessarily have the same area; the similarity theorems of Euclid become meaningless. In fact, Euclidean geometry is a limiting case of Lobachevskian geometry.

Nikolai Lobachevski

Another instance of a non-Euclidean geometry was given by BERNHARD RIEMANN, 1826–1866. He proposed a geometry, during the course of a famous lecture at the University of Göttingen in 1845, in which no line could be drawn parallel to a given line through a point outside that line. In this Riemannian geometry, the sum of the interior angles of a triangle is more than 2 right-angles, but tends to the Euclidean value as the area of a triangle tends to zero.

Bernhard Riemann

Both these non-Euclidean geometries are perfectly consistent systems, but our intuition tells us that they are not *true*, in the sense that the physical world around us seems to be Euclidean on the small scale at which we can measure it. However, intuition is by no means always a reliable guide. We should be careful before dismissing other geometries to remember that Euclidean geometry also is built upon definitions of things which have no counterpart in the physical world, for example, a *point*, defined as "that which has no part" (see page 9). We should remember too that Einstein's *Theory of Relativity* proposes that a generalized form of Riemannian geometry is true of physical space.

We return now to George Boole, whom we have already mentioned, and to the work on the algebra of logic with which the name of AUGUSTUS DE MORGAN, 1806–1871, is also associated; both published works in 1847.

Augustus De Morgan

Boole was primarily concerned with developing an *algebra of logic*. Using a form of algebra, different from ordinary algebra, he found that it was possible to deduce the whole theory of syllogism. Indeed, he was able to discuss errors in Aristotle's theory which had remained undetected for 2000 years. In *Unit 11, Logic I*, we remarked that what now goes by the name *Boolean Algebra* is really a later development of the algebra proposed by Boole. This development was the work of the logician, ERNST SCHRÖDER, 1841–1902, who started with Boole's system but then modified it to deal with certain difficulties which arose in interpretation, especially the interpretation of the *logical sum*.

Boole noticed that Aristotle's logic was dealing with *classes* of objects. The statement

All men are mortal

means that the class of all men is a sub-class of the class of all mortal beings. He denoted by

xy

the *logical product*, the sub-class of members of a class x which are also members of a class y. He denoted by

$1 - x$

the class of all objects not belonging to the class x. The class of all objects belonging to either class x or class y, x and y being assumed to have no members in common, was denoted by the *logical sum*,

$$x + y.$$

He wrote

$$x = 0$$

to denote that the class x is empty (that is, has no members), and

$$x = y$$

to denote that the classes x and y are identical.

Ernst Schröder

It is a comparatively easy exercise to verify the following:

$$xy = yx$$

$$x + y = y + x$$

$$(xy)z = x(yz)$$

$$(x + y) + z = x + (y + z)$$

$$x(y + z) = xy + xz.$$

These all correspond to familiar expressions in ordinary algebra. However, unlike ordinary algebra, it also follows that

$$xx = x$$

and

$$(x + y)(x + z) = x + yz.$$

A problem arose, however, with the logical sum when x and y had members in common. Boole allowed the use of

$$x + y$$

in this case during the working out of a problem, but as it was in such cases an "uninterpreted form", he required it to be suitably resolved in the final answer. We therefore do not find the expression

$$x + x = x$$

in Boole's system, since the left-hand side would be *for him* uninterpreted.

We can now give some examples of the uses of Boole's symbolic notation. For instance, if

x is the class of hard objects,
y is the class of elastic objects,

and

z is the class of metal objects,

then

xz represents the class of hard metal objects

and

$z(1 - y)$ represents the class of non-elastic metal objects.

The four basic propositions of Aristotle can be represented, for example, as follows:

All S is P	by	$s(1 - p) = 0,$
No S is P	by	$sp = 0,$
Some S is P	by	$sp \neq 0,$
Some S is not P	by	$s(1 - p) \neq 0.$

(The small letters s, p are used as the symbols corresponding to the classes S, P in Aristotle's logic.)

In Aristotle's logic, the syllogism:

> If all M is P
> and all M is S,
> then some S is P.

was considered valid. However, it becomes clear when the two premisses are put into Boole's symbolic notation as

$$m(1 - p) = 0$$

and

$$m(1 - s) = 0$$

respectively that nothing necessarily follows about S and P, since the equations are satisfied by $m = 0$, that is, by M being an empty class. Similarly, the Aristotelian syllogism:

> If no M is P
> and all M is S,
> then some S is not P,

which was also regarded as valid, is equally satisfied by M being empty. However, a weaker form of the first of these two syllogisms, namely:

> If some M is P
> and all M is S,
> then some S is P

is shown by Boole to be valid, since from

$$mp \neq 0$$

$$m(1 - s) = 0$$

it can be deduced that

$$sp \neq 0.$$

Boole concentrated his attention upon classes and the theory of syllogism, but his contemporary De Morgan was largely concerned with classes and with *relations* between classes. Many of their results were virtually identical, which with the hindsight we now possess is not at all remarkable, though it seemed to be so in their day. De Morgan's name is now associated with the *complementation laws*:

$$\overline{x \cap y} = \bar{x} \cup \bar{y}$$

$$\overline{x \cup y} = \bar{x} \cap \bar{y}$$

which we encountered in *Unit 11*, *Logic I*, but these and many of the other relations between classes were known in scholastic times, and merely restated by De Morgan in terms of a formal *algebra of classes*.

Boole and De Morgan were, as we have seen, principally concerned with expressing *already known* laws of reasoning and classification in terms of a symbolic algebra. The real founder of what we know today as *mathematical logic* was GOTTLOB FREGE, 1848–1925. It is to him that we owe very largely, not only the *propositional calculus* (see *Unit 11*), but also the proper use of the *universal* and *existential quantifiers* in mathematics, and the logical analysis of the important method of proof by *mathematical induction*.

Frege's principal aim was to try to found all arithmetic upon logic alone; that is, there were to be no statements about empirical facts. In this, he was really following Leibniz' dream of a universal symbolic language.

His approach was axiomatic, like that of Euclid, and he emphasized the distinction between *premisses* (which can be represented in symbolic form) and *rules of inference* (which cannot be written in symbolic form if one is confined to the symbols of the premisses).

Unlike Boole, Frege was unable to base his symbolism upon that of algebra because he was attempting to use logic to lay the foundations of arithmetic, and hence had to avoid any appearance of pre-empting what he was trying to derive. His greatest contribution lies in the exceptional precision of his scientific method in attempting to lay the foundations of mathematics.

In a very real sense, Boole, De Morgan and Schröder stand at the end of a long line going straight back to Aristotle. Frege, on the other hand, stands at the beginning of a new trend in logic which is continuing and which provides exciting lines of research at the present time.

At this point, it is necessary for us to look back in time and consider two crises in mathematics, one of which is still largely unresolved.

In the seventeenth and eighteenth centuries, mathematicians, struck by the power of calculus, had solved many problems which had hitherto been too difficult. In so doing, they had not always worried about the correctness of their methods, and some of their work can be described as cavalier, to say the least. For example, Euler employed in his work divergent series such as

$$1 - 1 + 1 - 1 + 1 - \cdots$$

which he summed by expressing it in the form

$$1 - x + x^2 - x^3 + \cdots$$

and letting $x = 1$. Finding that this series (a geometrical progression) has the limiting sum

$$\frac{1}{1 + x}$$

for $x < 1$, he concluded that the original series sums to $\frac{1}{2}$. Euler's method does not necessarily give consistent answers, however. For example, consider

$$\begin{aligned}\frac{1 + x}{1 + x + x^2} &= \frac{1 - x^2}{1 - x^3}\\ &= (1 - x^2)(1 + x^3 + x^6 + \cdots)\\ &= 1 - x^2 + x^3 - x^5 + x^6 - \cdots\end{aligned}$$

When $x = 1$ we again have the series

$$1 - 1 + 1 - 1 + 1 - \cdots$$

but this time Euler's trick would give us

$$\frac{1 + 1}{1 + 1 + 1} = \frac{2}{3}$$

as its limiting sum.

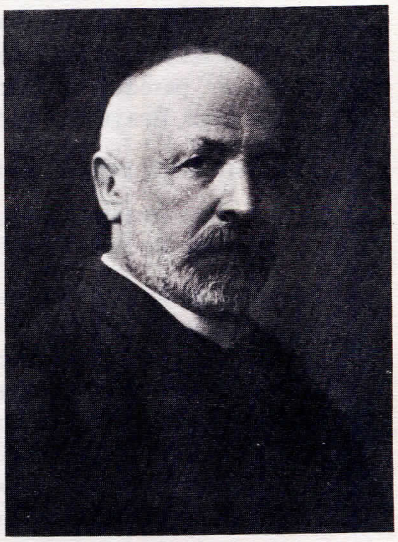
The crisis which arose out of the careless use of limiting procedures was overcome by AUGUSTIN LOUIS CAUCHY, 1789–1857, who showed how the cavalier methods of Euler could be replaced by the careful use of a theory of limits. This crisis was followed quickly by a much more difficult problem.

In the second half of the nineteenth century it had been shown that most of mathematics, as then known, could be reduced to a system constructed

Augustin Louis Cauchy

from the arithmetic of the positive integers. The irony of this is that, far from establishing the correctness and certainty of mathematics, it served only to reveal the pit over which much of it had been constructed. In developing more complicated systems from elementary arithmetic, a theory of sets is needed, and not merely a theory of sets of integers, but a theory that will embrace the concept of a set of sets, a set of sets of sets, and so on.

The creator of the *theory of sets* was GEORG CANTOR, 1845–1918. He suggested that the word *infinite* in mathematics has two meanings. First, it can stand for a magnitude which increases beyond any specified limit. This he called the *improper infinite*, and it was represented by the now familiar symbol ∞. The second meaning can be illustrated by considering a *finite* line as an infinite collection of points. Because the line is finite, there is a sense in which we can think of this collection as a *completed infinite*. (The line can be drawn in its entirety even though it contains an infinite number of points, but an increasing magnitude cannot be represented by any complete figure.)



Georg Cantor

Cantor's definition of a set as "any collection into a whole of definite and separate objects" gives rise to no difficulty so long as we are considering only a finite number of things. Problems do arise, however, in connection with infinite sets, and, in particular, with the *set of all sets*.

Cantor called two sets *equivalent* if they can be put into *one–one correspondence*; thus the sets $\{a, b, c, d, e\}$ and $(1, 2, 3, 4, 5\}$ are equivalent since we have, for example, the correspondence:

$$a \longleftrightarrow 1$$
$$b \longleftrightarrow 2$$
$$c \longleftrightarrow 3$$
$$d \longleftrightarrow 4$$
$$e \longleftrightarrow 5$$

It is clear that equivalent sets must have *the same number of elements*, and no paradox arises so long as we confine ourselves to *finite* sets.

Now consider the set of positive even integers, a subset of the set of all positive integers. These can be put in one–one correspondence with the set of all positive integers, for example:

$$2 \longleftrightarrow 1$$
$$4 \longleftrightarrow 2$$
$$6 \longleftrightarrow 3$$
$$8 \longleftrightarrow 4$$

and generally,

$$2n \longleftrightarrow n$$

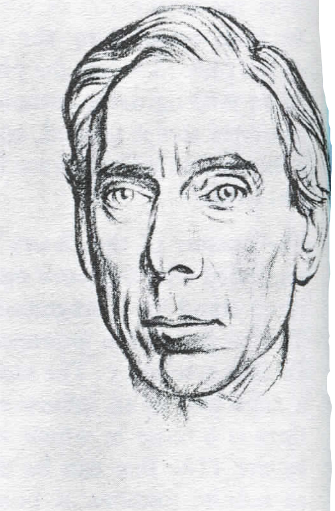
So there are just as many positive even integers as there are positive integers. There are many such examples of a set having the same number of elements as a proper subset of itself, but in every such case the number of elements is infinite. What then has happened to Euclid's common principle:

> The whole is greater than the part

(see page 9)? It clearly does not hold for infinite sets. In fact, we could *define* a *finite set* as one which cannot be made equivalent to a proper subset of itself, and an *infinite set* as one which can.

However, we must not imagine that with Cantor's set theory, all the problems and paradoxes were solved. To demonstrate that this was not so, we mention just one of the difficulties of Cantor's theory.

If we call *normal* those sets which do not contain themselves, and *abnormal* those which do (such as the set of all sets), we can ask whether the *set of all normal sets* is normal or abnormal. Suppose it is *normal.* By definition it does not contain itself. But, as the set of *all* normal sets, it does contain itself. Now suppose it is *abnormal.* Then it does contain itself and so it must be normal. In either case we arrive at a contradiction. (This particular paradox is known as *Russell's paradox* after the English philosopher, BERTRAND RUSSELL, 1872–1970, who discovered it.)


Bertrand Russell

There are many popular forms of this paradox. One such is the following:

> In a certain village, the barber shaves all those and only those who do not shave themselves. Does he therefore shave himself?

Suppose the barber does shave himself. Then it follows that he does not, since he shaves only those who do not shave themselves. Suppose now that he does not shave himself. Then he does shave himself, since he shaves all those who do not shave themselves! We can get round such a popularization of Russell's paradox simply by concluding that the result proves that the postulates are false, that is, that there can be no such barber. There are, however, normal and abnormal sets, so the way round Russell's paradox itself is not clear, although there must be either a mistake in the reasoning or a looseness in the definitions.

The work of Frege, which we have briefly discussed (see page 15), strongly influenced Russell, who, together with ALFRED NORTH WHITEHEAD, 1861–1947, produced the three-volume *Principia Mathematica.* Russell and Whitehead consciously followed Frege's general principles but adopted changes in his symbolism and nomenclature. We shall not discuss these changes; we shall concentrate on the way in which they proposed to avoid the difficulty of Russell's paradox.

Alfred North Whitehead

We begin by giving a definition of the number 1 which is, in effect, an interpretation of that of Russell and Whitehead expressed in modern notation:

$$1 = \{X : \sim (X = \varnothing) \text{ and } y \in X \wedge z \in X \Rightarrow y = z\}.$$

We read this as:

> "the number ONE is the set of objects X such that no X is empty, and such that if y and z both belong to the same X, then y and z are one and the same."

Notice particularly that each X must be itself a set (since we are told something about members of X and also that no X is empty), and that consequently 1 is being defined as a *set of sets.* In fact, 1 is simply being defined as the *set of all sets having a single member*. This may seem at first sight to be a somewhat involved definition, but it is not really so. It agrees very well with the way in which we are introduced to numbers in everyday life. To have produced such a definition was a very great achievement, since it had previously been thought that the positive integers were something which could not be analysed further. LEOPOLD KRONECKER, 1823–1891, made the famous remark:

> God made integers, all else is the work of man.*

But even the definition above is not without its difficulties. It is couched in terms of a set theory, but this cannot be the set theory of Cantor, since the latter contains the very paradox which the definition is designed

* *Jahresberichte der Deutschen Mathematiker Vereinigung, Bd. 2, page 19.*

to avoid. Whitehead and Russell decided that the root cause of the trouble lay in allowing anything to belong to itself. So they proposed a *theory of types.*

> *Individuals* were said to be of *type* 0,
> *sets of individuals* were said to be of *type* 1,
> *sets of objects of type* 1 were said to be of *type* 2,
> and so on.

Expressions such as

$$y \in X$$

were allowed only if X was of a type exactly one higher than y. This avoids the difficulties of Russell's paradox, but whether or not other difficulties appear is not so clear.

Going back to the definition of the number 1 as a set of sets, and accepting the theory of types, we find that we do have a serious problem: y, z must be of the same type and X must, therefore, be one type higher. Clearly, 1 as a set of X's is of type one higher again. According to our choice for the y's and z's we could define numbers of type 2, 3, 4, etc., but this was not what was intended at all. What would it mean if we attempted to add the 1 of type 2 (say) to that of type 3? The intention was to define a unique number 1.

Whitehead and Russell decided to cut their way out of this tangle by introducing what they called the *axiom of reducibility*. This axiom means (roughly) that if we define a mathematical object of a certain type, then we may assume the existence of corresponding objects of every other type. We can think of the general drift of this as being:

> although types are important sometimes,
> we can ignore them most of the time.

Obviously, such an assumption allows the possibility of inconsistency occurring again. The attempt to base mathematics on an unshakeable logical foundation is apparently not viable. The need for an axiom such as the axiom of reducibility was a major factor in the disillusionment of mathematicians with the Whitehead–Russell system.

The failure of the attempts to derive mathematics from logic highlights a major mathematical problem of the twentieth century; however, other attempts were made to clarify the severe problems arising in the foundations of mathematics.

A completely different approach was that of the Dutch mathematician, L. E. J. BROUWER, 1881–1968; Brouwer pioneered what has come to be known as the *intuitionist school* of mathematicians. The name is perhaps a little unfortunate, since it seems to imply that there was an appeal to intuition in the course of mathematical proofs. In fact, the proofs of the intuitionists are at least as rigorous as those of other mathematicians; often, they demand much greater logical precision. The name comes from the fact that the intuitionists reject any attempts to base elementary arithmetic on some more fundamental system, and regard the positive integers as an intuitive reality serving as a sure basis on which to build. There is much to be said in favour of this point of view.

Brouwer saw the idea of *existence* in mathematics as synonymous with *constructibility*, and *truth* as synonymous with *provability*. So to assert the *truth* of a mathematical statement is to assert that *we have a proof of it.* Similarly, to assert the *falsehood* of a mathematical statement means that we have a proof that *if we assume the statement to be true this will involve us in a contradiction.* This has important logical implications.

In *Unit 11, Logic I*, we saw that for any proposition **a**,

$$\mathbf{a} \vee \sim\mathbf{a}$$

is a *tautology*. This tautology, known from ancient times as *the law of excluded middle*, in effect states that a given proposition must be *either* TRUE *or* FALSE. For an intuitionist it means that "either we have a proof of **a** or else we have a proof that the assumption of **a** leads to a contradiction". The law of excluded middle cannot therefore be included in the intuitionist system, since it implies that there is no such thing as an unsolved problem. The effect of the intuitionist assumptions is that whole areas of classical mathematics have to be rejected where traditional proofs based on the assumption

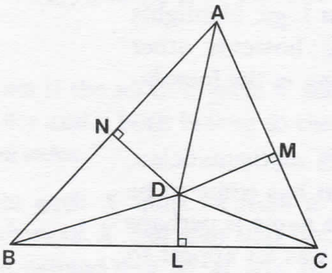
$$\mathbf{a} \vee \sim\mathbf{a}$$

cannot be reconstructed on an intuitionist basis. Most mathematicians would agree that anything proved in the intuitionist system is valid, but it is generally thought that the intuitionists are over-cautious, and that their rejection of so much otherwise acceptable mathematics is a serious drawback.

We turn now to the founder of yet another school of thought. DAVID HILBERT, 1862–1943, considered that the attempt to base mathematics entirely upon logic was far too ambitious. His approach was to break down the various problems into parts, and tackle them piecemeal. Initially, the question of truth and falsehood, which had always caused philosophical difficulties, was to be laid on one side, and concentration was to be on the *consistency* and the *completeness* of sets of axioms. In this context consistency implies that in any system one cannot prove both a result and the contradiction of that result. Completeness means that sufficient axioms have been given so that all the results which ought (in some sense) to be deducible actually can be deduced.

One of Hilbert's earliest achievements was to formulate a complete set of axioms for Euclidean geometry. Consider the following Euclidean proof:

Let ABC be any triangle:



Let the bisector of the angle at A and the perpendicular bisector of BC meet at D. Drop perpendiculars DM, DN on to AC, AB respectively. Join DC, DB. Let L be the mid-point of BC. Now, since $BL = LC$, DL is common, and $B\hat{L}D = C\hat{L}D = 90°$, triangles BLD, CLD are congruent, and so $BD = CD$. Since angles $N\hat{A}D$, $M\hat{A}D$ are equal, $A\hat{N}D = A\hat{M}D = 90°$, and AD is common, triangles AND, AMD are congruent, so $DN = DM$, $AN = AM$.

Since $DN = DM$, $BD = DC$ and $B\hat{N}D = C\widehat{M}D = 90°$, triangles BND, CMD are congruent, so $NB = MC$.

Since

$$AN = AM \quad \text{and} \quad NB = MC,$$

it follows that

$$AB = AC.$$

So an arbitrary triangle is isosceles; hence every triangle is isosceles.

This is clearly nonsense, yet the proof follows from Euclid's axioms for geometry. The difficulty lies in the fact that *Euclid's axioms are incomplete* and need to be supplemented by *axioms of incidence* stating that, when lines are drawn in a certain way, they intersect in a certain part of the plane. (The way we drew the figure presumed and subsequently argued that D lies inside the triangle — an unjustified assumption.)

Because Hilbert and his followers concentrated on the construction of formal systems by means of which they could separately investigate each individual branch of mathematics, their approach came to be known as *formalism.* In order to be able to examine the consistency and completeness of each of these formal systems, their programme included the construction of a more general language, or *metalanguage*, in which the formal systems could be discussed. Ultimately, the consistency of the formal systems was shown to depend upon the consistency of elementary arithmetic.

Unfortunately, as had happened with all other systems which preceded it, Hilbert's programme eventually received a serious set-back. This happened when in 1930 KURT GÖDEL, 1906–, announced his results concerning doubtful propositions in a formal system.

Kurt Gödel

Gödel showed that in any system "rich" enough to express elementary arithmetic, either there will be sentences proved which are *false*, or there will be unprovable sentences which are *true*, where *false* and *true* have to be given an interpretation according to the system concerned. This is probably the greatest of all results in modern logic. To obtain some idea of its significance, we shall consider a simple formal system.

Suppose that we start with a formal system involving (say) one or two logic symbols, a few arithmetic symbols like 0, 1, +, =, and some axioms and rules of transformation. It is conceivable that all the sentences possible in such a system could be written down. Now our system must not be "rich" enough to include paradoxes such as the *liar paradox* (see page 8) or it would be inconsistent. Suppose, however, that it does contain a sentence of the form:

This sentence is not provable.

We shall call this sentence S.

If S is *true*, then S is not provable.
If S is not *true*, then S is provable.
If S is provable, then S is not *true*.
If S is not provable, then S is *true*.

So we have to conclude that if our system is "rich" enough to include S, then it must include at least one sentence which is *true* if and only if it is not provable. This difficulty arises in all systems "rich" enough to include elementary arithmetic, so the formalist approach is in the end shown to be just as untenable as the programme for deriving all mathematics entirely from logic. It would now appear that *no such system can be both consistent and complete.*

In our "history" we have tried to show how mathematics and logic have repeatedly interacted throughout their respective developments. Each time there has been direct interaction both disciplines have benefitted. Many problems have been solved, but the resolution of the problems of one century has invariably thrown up others which have had to be tackled by the logicians and mathematicians of the next. We may now ask the question: "Where do we stand?", since there still seem to be unresolved paradoxes at the foundations of mathematics. The situation can probably be described something like this:

If we want absolute certainty, then we shall have to be content to restrict ourselves to a very "trivial" system such as a propositional calculus (as discussed in *Unit 11*) with a finite number of propositions. If, however, we want to be able to enjoy the richness of the adventures into reason which the concepts of *set theory* and *number* allow, then we shall have to accept some element of insecurity, and the possibility of being faced with a paradox which only a journey further afield into (possibly) even more insecure surroundings can resolve.

17.2 PROOF IN MATHEMATICS

17.2

17.2.0 Introduction

17.2.0

Introduction
* * *

In section 17.2 our aim is to set out the general framework in which a mathematical proof is possible, and then to examine the various kinds of proof which are common to all branches of mathematics. We shall illustrate the arguments with a number of examples.

Nothing in section 17.1 is essential for your understanding of the remainder of this text. Where concepts arise which have been discussed in section 17.1, we shall give sufficient explanation for any back-reference to be unnecessary.

In the study of mathematics *it is not possible to avoid proof*, and once we are faced with the problem of proving a mathematical conjecture we are in a situation where mathematics and logic are both involved. If our mathematics is "wrong" in the sense that we select axioms which are unsuited to our particular purposes, then, however correct our logical inferences, it will be a stroke of remarkable luck if we arrive at the "right" conclusion. Equally, if our mathematical starting point is "right", but our logical processes are invalid, the chances of arriving at a "right" conclusion by sheer accident are very slender.

So, if we are to be able to prove mathematical conjectures, we need to start in the "right" place and travel strictly according to the "right" rules. In this section we shall be concerned principally with a discussion of such rules.

17.2.1 The Ingredients for Proof

17.2.1

Discussion
* * *

A system of mathematics must, like everything else, begin somewhere. We might be tempted to think that our starting point is a number of *definitions*; for example, we could take as our starting point the definition of *set* as follows:

> A *set* is a collection of distinct well-defined objects.

However, in writing down this definition we have used a number of terms: *collection, distinct, well-defined, object.* We are, in fact, presuming that these terms are already understood. If that presumption is to be justified, then these terms must in turn have been either defined or presumed. We can, of course, provide definitions of all four words, but we shall find if we do so that we are using other words, which will in their turn require definition unless they are presumed, and, sooner or later, we shall find ourselves in a circular situation. So it appears that before we can produce definitions, we need to presume certain terms. Such presumed terms are called primitive terms, and without them there is no point at which we can make a beginning.

Definition 1†
* *

(Notice also that it is extremely difficult to write down even our definitions without recourse to some kind of language in which we can talk about our terms, and subsequently discuss whatever mathematical system we choose.)

As examples of primitive terms we take *point* and *line* in plane geometry. Euclid defined a *point* as

> that which has no part,

and a *line* as

> a breadthless length,

† Circular Situation 1.

but these definitions simply rely on the terms *part*, *breadth*, *length*, which Euclid did not attempt to define.

Suppose, then, that we accept *point* and *line* as primitive terms; we can then define, for example, a *line segment* as

> that part of a line contained between two given points on a line,

but even this presumes such terms as *part*, *contained*, *two*, *given*, as well as a general framework of English.

This may all seem pedantic, and in practice we get along very well for most of the time presuming a great number of terms and a large number of variations of English grammar. But every now and then we get into difficulties because we have not realized that some of our presumptions are mutually incompatible. We need to be quite sure just *what we are accepting as primitive terms*, and to take care that we do not go outside this framework in formulating our definitions.

Having decided upon our primitive terms and definitions, we next require a set of axioms (or postulates). An axiom is a statement about objects (which have been defined) which is *assumed to be true* (in what ever sense we may decide to interpret the word *true*).

Definition 2
* * *

Conceivably, our choice of axioms can be absolutely arbitrary, but, in general, we tend to rely on intuition or on our experience of the physical world. An example of an axiom is provided by Euclid's famous *parallel postulate*, which may be stated in the form:

> Through a point outside a given line there can be drawn only one line parallel to the given line.

An axiom is said to be independent within a system if it cannot be deduced from other axioms of the system. For many years mathematicians tried unsuccessfully to show that the parallel postulate could be deduced from other Euclidean axioms and was, therefore, not independent. Eventually, geometries were invented in which the postulate did not hold, although previously it had always been regarded as a self-evident truth.

Definition 3
* *

In *Unit 11*, *Logic I* we defined a proposition as a statement which must be *either* TRUE *or* FALSE. We represent this by, for example, **a** or ~**a**, and this corresponds to an axiom of deductive reasoning (known as the *law of excluded middle*).

Much of our mathematical activity consists of deducing *theorems* from axioms and definitions. A theorem may be defined as a *valid deduction* from a set of axioms and definitions; but this definition begs the question, since in order to determine whether or not a given deduction is *valid*, we need to have a set of *rules of inference*. If it had been possible to deduce the parallel postulate validly from Euclid's other axioms, this would have shown that, strictly, the postulate was a theorem and not an axiom. (We use the word "strictly" here, because we do in fact quite often adopt sets of axioms for convenience where one or more of the axioms is not independent.)

Definition 4
* * *

A set of axioms is said to be consistent if it is not possible to deduce contradictory propositions from them by a valid deductive process. Clearly, we want any set of axioms to be consistent. An example of a likely inconsistency occurs if we try to include the (apparently obvious) axiom:

Definition 5
* *

> The whole is greater than the part,

when we are dealing with infinite sets. For example, the set of all positive even integers can be put in one–one correspondence with the set of all positive integers as follows:

$$2 \longleftrightarrow 1,$$
$$4 \longleftrightarrow 2,$$
$$6 \longleftrightarrow 3,$$
$$8 \longleftrightarrow 4,$$

and generally,

$$2n \longleftrightarrow n.$$

Since we define the number of elements in a set by means of a one–one correspondence with the set of positive integers, it follows that there are just as many even positive integers as there are positive integers, and yet the set of all even positive integers is a proper subset of the set of all positive integers.

The *rules* by means of which *we deduce theorems from axioms*, called the rules of inference, need to be carefully stated. History has shown how quite developed mathematical and logical structures can eventually collapse because these rules have been broken. We shall look at the important rules of inference in the section which follows. Before doing so, we shall briefly discuss one or two other ingredients which we use continually in mathematics.

Definition 6
* *

In *Unit 11*, *Logic I*, we discussed the concept of a proposition and a corresponding algebra (calculus) of propositions. Let us now consider the question:

Is an *equation* a proposition?

For example, is

$$x^2 - 4 = 0$$

a proposition? Before answering this question, let us look at a similar kind of expression in ordinary sentence form:

x is a Frenchman.

This can be interpreted in (at least) two ways. There is a sense in which it asserts that the 24th letter of the alphabet is a Frenchman. This is a *proposition*, and, what is more, it is FALSE. However, in another sense, it can be regarded as an *incomplete sentence*, which, until the symbol x is replaced by a defined term, we cannot assert to be either TRUE or FALSE. Such an *incomplete sentence* is called an open sentence, and it becomes a proposition only when the *variable* x is replaced by a *defined term*. In this sense, the open sentence:

Definition 7
* * *

x is a Frenchman

can be converted into a proposition by the substitution of (say) Jean Brun for x.

Let us look again at the equation

$$x^2 - 4 = 0.$$

In terms of our discussion of

x is a Frenchman

we can now see that the equation is an *open sentence* and not a proposition. If we substitute for x a defined (or primitive) term from the particular set in which we are reasoning,* then we may have, say,

$$6^2 - 4 = 0$$

* The set of all words and symbols to be accepted as usable in a given argument is called the universe of discourse or the universal set.

or

$$(-2)^2 - 4 = 0,$$

the former being a FALSE proposition and the latter being a TRUE proposition.

We call the set of all defined terms which may be substituted for the variable in an open sentence so as to give TRUE propositions, the truth set of the open sentence. Thus the truth set of

Definition 8
* * *

x is a Frenchman

is the set of all (living) Frenchmen, and the truth set of

$$x^2 - 4 = 0$$

is the set $\{2, -2\}$, assuming that these are defined or primitive terms. So, solving an equation in mathematics amounts to the logical process of determining the truth set of an open sentence. (The *truth set* is the same as the *solution set* in the context of *Unit 6, Inequalities.*)

At this point it is useful to introduce the two quantifiers which we use both in logic and in mathematics. These are known as the universal quantifier and the existential quantifier, and they correspond respectively to prefixing an open sentence containing the variable x with

for all x (universal quantifier)

Definition 9
* * *

and

there exists an x such that (existential quantifier).

Definition 10
* * *

(Alternatively, we may read the existential quantifier as

for some x,

where *some* is taken to mean at least one.) Let us look at some examples.

First, the assumption that our equation

$$x^2 - 4 = 0$$

has a solution (or solutions), gives it an implied quantifier, the existential quantifier. We use the symbol $\exists_x$ for this quantifier, and so we write:

Notation 1
* * *

$$\exists_x x^2 - 4 = 0,$$

which we read as:

there exists an x such that $x^2 - 4 = 0$.

This is now a proposition asserting that the truth set of the open sentence:

$$x^2 - 4 = 0$$

is *not empty*. We have assumed here that our universe of discourse has already been adequately defined. In mathematics, in order to make each statement precise, we often specify the universe of discourse by including expressions such as

$$x \in R, \qquad x \in Z^+.$$

We could thus write:

$$\exists_x x^2 - 4 = 0 \qquad (x \in R).$$

We have usually done this in our mathematical expressions in the units so far, and we shall continue to do so, since it is an extremely important safeguard against possible error and misunderstanding. Notice, for example, that the truth set of

$$x^2 - 4 = 0 \qquad (x \in R)$$

is *not* the same as that of

$$x^2 - 4 = 0 \qquad (x \in Z^+),$$

and that

$$\exists_x x^2 - 4 = 0 \qquad (x \in \{1, 3, 5, 7, \ldots\})$$

is FALSE, whilst

$$\exists_x x^2 - 4 = 0 \qquad (x \in \{2, 4, 6, 8, \ldots\})$$

is TRUE.

As a second example, consider

$$x^2 - 2x + 1 = (x - 1)^2 \qquad (x \in R).$$

Notation 2 * * *

This has an implied quantifier, the universal quantifier, since the expression is an *identity*. We use the symbol $\forall_x$ for this quantifier, so we write:

$$\forall_x x^2 - 2x + 1 = (x - 1)^2 \qquad (x \in R)$$

which we read as

for all x, $x^2 - 2x + 1 = (x - 1)^2$, where x is a real number.

This is now a proposition asserting that the truth set of the open sentence

$$x^2 - 2x + 1 = (x - 1)^2 \qquad (x \in R)$$

is the set of real numbers. When we write our expressions in full, including the appropriate quantifier, there is no difficulty in distinguishing between an *equation* and an *identity*.

Digression * *

At first sight, it might be thought that whenever an open sentence prefixed by the universal quantifier is a TRUE proposition, then the same open sentence prefixed by the existential quantifier will also be a TRUE proposition. If we accept

All men are mortal

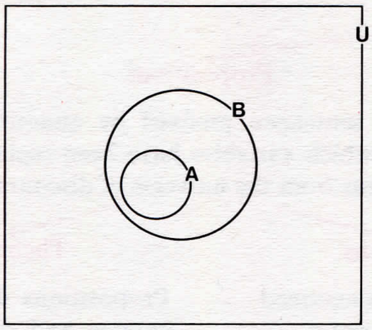
as TRUE, then it seems that

Some men are mortal

is TRUE in the sense that at least one man is mortal. Similarly, if we think in terms of sets and Venn diagrams, we can have:

$$A \subset B,$$

that is, *each* element of set A is an element of set B, represented by:



It would appear that since

some element of set A

refers to a subset of A, it must necessarily follow that

Some element of set A is an element of set B

is TRUE. In fact, the deductions are all correct provided that A is not the empty set. The use of the universal quantifier does not necessarily imply that the universe of discourse is not empty. The existential quantifier, however, specifically asserts that *there exists* some x having a given property. Thus we may accept as TRUE the proposition:

$$\forall_x x \text{ is bright green} \quad (x \in \text{the set of flying elephants}),$$

but we cannot deduce from this the proposition:

$$\exists_x x \text{ is bright green} \quad (x \in \text{the set of flying elephants}),$$

since the set to which x belongs is the empty set. You may think again that we are being pedantic, but the point appears trivial only because it is made in everyday terms — such an error would not be so obvious in the middle of a complicated piece of mathematics. This is a difficulty which has actually arisen in the course of logical arguments, and (if it does nothing else) it serves to underline the importance of clearly stating our universe of discourse.

Discussion
* *

Definition 11
* * *

The proof that propositions including the existential quantifier are TRUE plays an important role in mathematics, and such TRUE propositions are called existence theorems. Notice particularly that *proving an existence theorem* is to be distinguished from *determining the truth set of an open sentence.* To prove that an equation has a solution is not the same as finding the actual solution itself It is often very important, before expending a great amount of time and ingenuity trying to solve a problem, that we should try to find out whether a solution does in fact exist.

Summary
*

We summarize the main ingredients of a proof:

UNIVERSE OF DISCOURSE

Primitive Terms

Terms whose meanings are presumed without definition.

Defined Terms

Terms which are defined in terms of primitive terms.

Note: The universe of discourse includes words and symbols.

SENTENCES

Open Sentences

Sentences which are incomplete in that they include variables.

Propositions

Open sentences, prefixed by quantifiers, or in which variables have been replaced by terms from the universe of discourse.

Axioms

Propositions assumed without proof.

Theorems

Propositions deduced from axioms and definitions by rules of inference.

RULES OF INFERENCE

The means by which we validly deduce theorems from axioms and definitions (see 17.2.2).

Analogy *

We can think of an analogy with the game of chess. The pieces have to start in a certain given arrangement on the board, and are then subsequently moved according to a set of prescribed rules. These rules not only state, for example, that the piece called a castle can only move parallel to the sides of the board, but they also include certain more basic statements such as "not more than one piece can occupy any one square at the same time". The analogy is:

32 white squares 32 black squares 16 white pieces 16 black pieces	⟷	Universe of discourse
Arrangement of squares Allowable positions of pieces Initial positions	⟷	Axioms
Rules for moving pieces	⟷	Rules of inference
Subsequent positions of pieces	⟷	Theorems

Exercise 1

Exercise 1

(i) Rearrange the following in a correct hierarchy of "primitiveness": (1 minute)

defined term,
theorem,
axiom,
primitive term.

(ii) What is wrong with the following argument? (2 minutes)

$1 + 3$ contains a plus
and $1 + 3 = 4$,
therefore 4 contains a plus.

(iii) Which of the following are *open sentences* and which are *propositions*? Which (if any) are suitable as axioms? (2 minutes)

(a) $x + 3 = 7$ $(x \in R)$
(b) $\exists_x x + 3 = 0$ $(x \in Z^+)$
(c) $\forall_x x = x$ $(x \in R)$
(d) $\mathbf{a} \vee \sim\mathbf{a}$ ($\mathbf{a} \in P$, the set of propositions)
(e) $\mathbf{a} \wedge \mathbf{b} \Rightarrow \mathbf{c}$ $(\mathbf{a}, \mathbf{b}, \mathbf{c} \in P)$. ■

Solution 1

Solution 1

(i) primitive term — defined term — axiom — theorem.

(ii) The universe of discourse is not made clear.

1 + 3 contains a plus

is a proposition about the arrangement of the *symbols* 1, +, 3, whereas the proposition

$$1 + 3 = 4$$

is a proposition about the *numbers* 1, 3, 4.

(Note: This highlights the distinction between the *mention* of a term and the *use* of a term.)

(iii) (a) Open sentence.
(b) Proposition. (Do not be confused by the fact that it is FALSE.)
(c) Proposition. Suitable as an axiom.
(d) Proposition. Suitable as an axiom.
(e) Open sentence. ■

17.2.2 Rules of Inference

17.2.2

Main Text
* * *

In this section we look at the more important *rules of inference* by means of which we are able to deduce theorems from a set of axioms and definitions.

Rule of Detachment
* *

The first of these is known as the rule of detachment (or *modus ponens*). This rule states:

For any propositions **a**, **b**,

from **a** is TRUE
and **a** ⇒ **b** is TRUE,
we infer that **b** is TRUE.

For example, if we accept as TRUE the two propositions:

It is raining
If it is raining then I will stay at home,

then we infer that the proposition:

I will stay at home

is TRUE.

We can easily justify the acceptability of the rule of detachment by looking again at the truth table for the connective ⇒, which we discussed in detail in *Unit 11*, *Logic I*.

The truth table is:

a	**b**	**a ⇒ b**
0	0	1
0	1	1
1	0	0
1	1	1

(Remember that 0 represents FALSE, and 1 represents TRUE.) The only row corresponding to both **a** and **a** ⇒ **b** being TRUE is the bottom row, and in this row **b** is also shown to be TRUE.

Rule of Syllogism
* *

The second rule is known as the rule of syllogism. This rule is an expression of the transitivity of the conditional connective ⇒ which we discussed in *Unit 11*, *Logic I*. This rule states:

For any propositions **a**, **b**, **c**,

from **a** ⇒ **b** is TRUE
and **b** ⇒ **c** is TRUE,
we infer that **a** ⇒ **c** is TRUE.

For example, if we accept as TRUE the two propositions:

$\forall_x$ if x is odd, then x is not divisible by 4 $(x \in Z)$
$\forall_x$ if x is not divisible by 4, then x is not divisible by 16 $(x \in Z)$

then we infer that the proposition:

$\forall_x$ if x is odd, then x is not divisible by 16 $(x \in Z)$

is TRUE.

The transitivity of the conditional is justified by the fact that

$$[(\mathbf{a} \Rightarrow \mathbf{b}) \wedge (\mathbf{b} \Rightarrow \mathbf{c})] \Rightarrow (\mathbf{a} \Rightarrow \mathbf{c})$$

is a *tautology*; that is, it is necessarily TRUE whatever the truth values of **a**, **b**, **c** (see *Unit 11*, Exercise 11.1.7.1).

Rule of Equivalence
★★

The third rule is known as the rule of equivalence. The rule states:

> At any stage of an argument we can replace any proposition by an equivalent proposition, and in any proposition we can replace any term by an equivalent term.

For example, instead of the proposition $\mathbf{a} \Rightarrow \mathbf{b}$ we can substitute $\sim\mathbf{a} \vee \mathbf{b}$. (See *Unit 11*, section 11.1.3.)

It is this rule which enables us to translate our investigations from one system to another in which the proof or the computation is more convenient, and thus provides us with a justification of the *modelling* process by which we investigate physical problems in terms of their corresponding mathematical models.

Rule of Substitution
★★

The rule of equivalence is sometimes known as the rule of substitution, but we reserve this latter name for the following rule, which is very important in mathematical reasoning:

> In any TRUE proposition, we can replace a symbol representing an arbitrary element of a non-empty set by one representing a specific element of the same set.

This rule permits us to argue validly from the TRUE proposition that a particular property holds for an *arbitrary* element of a set (that is, for *all* elements of a set), to the proposition that the same property holds for a *specific* element of that set. For this reason, it is sometimes abbreviated to:

> What is TRUE of *all*, is TRUE of *one*.

We have already discussed (page 28) the fallacy of arguing from *all* to *some* if the set of elements concerned is empty, so we have been careful in our version of the rule to specify a *non-empty* set, in order to avoid falling into a similar error.

We can now argue validly from

$\forall_x x$ is mortal $\quad (x \in$ the set of all men$)$

to

John Smith is mortal,

since John Smith is a specific member of the set of which x is an arbitrary element.

Similarly, we can argue from

$$\forall_x (x - 1)(x + 1) = x^2 - 1 \qquad (x \in R)$$

to

$$99 \times 101 = 100 \times 100 - 1 = 9999.$$

Before considering how these rules are used in some specific proofs, we summarize them as follows:

Summary
★★★

Rule of detachment

From **a** and $\mathbf{a} \Rightarrow \mathbf{b}$ are TRUE, we infer that **b** is TRUE.

Rule of syllogism

From $\mathbf{a} \Rightarrow \mathbf{b}$ and $\mathbf{b} \Rightarrow \mathbf{c}$ are TRUE, we infer that $\mathbf{a} \Rightarrow \mathbf{c}$ is TRUE.

Rule of equivalence

Equivalent propositions/terms may be substituted for each other.

Rule of substitution

What is TRUE of an arbitrary element of a non-empty set is TRUE of a specific element of the set.

Examples
★ ★

In the examples which follow, we do not start at "rock bottom" with primitive terms, definitions and axioms, since this would be a somewhat lengthy and tedious business. We have to start, therefore, either with propositions which have been previously deduced or are deducible from the axioms of the system in which we are arguing, or by making some special assumption to give us a starting point for our argument. Such assumed propositions are called hypotheses.

Definition 1
★ ★

Example 1

Example 1

(Assume a universe of discourse to be defined throughout.)

GIVEN $\forall_x \quad x \in A \Rightarrow x \in B$

$\forall_x \quad x \notin C \Rightarrow x \notin B$

$\forall_x \quad x \in C \Rightarrow x \in D$

TO PROVE $\forall_x \quad x \in A \Rightarrow x \in D$

$$\begin{array}{llll}
\text{PROOF} & & x \in A & \text{(hypothesis)} \\
& \forall_x & x \in A \Rightarrow x \in B & \text{(given)} \\
& \therefore & x \in B & \text{(rule of detachment)} \\
& \forall_x & x \notin C \Rightarrow x \notin B & \text{(given)} \\
\therefore & \forall_x & x \in B \Rightarrow x \in C & (\text{rule of equivalence}: \mathbf{b} \Rightarrow \mathbf{c} \text{ is equivalent to } \sim\mathbf{c} \Rightarrow \sim\mathbf{b}) \\
& \therefore & x \in C & \text{(rule of detachment)} \\
& \forall_x & x \in C \Rightarrow x \in D & \text{(given)} \\
& \therefore & x \in D & \text{(rule of detachment)} \\
\text{i.e.} & \forall_x & x \in A \Rightarrow x \in D &
\end{array}$$

Q.E.D. ■

Example 2

Example 2

GIVEN A set S on which is defined a closed binary operation $\circ$.
An element $e \in S$, is called an *identity element*, if it satisfies:

$$\forall_x \quad x \circ e = e \circ x = x \qquad (x \in S).$$

TO PROVE If e_1 and e_2 are identity elements for S, then $e_1 = e_2$.

$$\text{PROOF} \quad \left.\begin{array}{ll} \forall_x \quad e_2 \circ x = x & (x \in S) \\ \forall_x \quad x \circ e_1 = x & (x \in S) \end{array}\right\} \text{(given definition of identity element)}$$

$$\text{and} \quad \left.\begin{array}{l} \therefore \quad e_2 \circ e_1 = e_1 \\ \quad e_2 \circ e_1 = e_2 \end{array}\right\} \text{(rule of substitution)}$$

$$\therefore \quad e_1 = e_2 \qquad \text{(rule of equivalence).}$$

Q.E.D. ■

Definition 2
* *

Both Examples 1 and 2 are instances of what we call direct proof, that is to say, they proceed by a series of steps, each step using a rule of inference, from what is given or assumed to what is to be proved.

Definition 3
* *

An alternative type of proof, known as indirect proof proves a proposition which is *equivalent* to what is to be proved. You can easily see, therefore, that the *rule of equivalence* enables us to convert an *indirect proof* to a *direct proof* by the addition of one further step in the chain of reasoning. You may wonder why we bother to make any distinction between direct and indirect proof. The problem arises only when there is disagreement as to which propositions are indeed equivalent to one another.

The most common form of indirect proof in mathematics involves proving that a proposition, contradictory to what we want to prove, is FALSE, by first assuming it to be TRUE, and then proving that this assumption leads to a contradiction. In other words, if we want to prove that **a** is TRUE, we prove that

$\sim\mathbf{a}$ is FALSE,

and we then infer that

a is TRUE.

(We discuss this kind of proof in section 17.2.4.)

Exercise 1

Exercise 1

(i) What can be inferred from the truth of: (1 minute)

Eggs cost 40p per dozen.
If eggs cost 40p per dozen, then eggs are expensive.

Which rule of inference did you use?

(ii) List three propositions which are equivalent to the proposition: (4 minutes)

$\mathbf{a} \Rightarrow \mathbf{b}$

Justify each by reference to truth tables.
(Note: Use only **a**, **b**, $\sim$, $\vee$, $\wedge$, $\Rightarrow$.)

(iii) For the following proof, indicate the justification for each line:* (3 minutes)

GIVEN 2 does not divide x $(x \in Z^+)$.
A prime divisor of the product of two integers divides at least one of them.
TO PROVE 2 does not divide x^2 $(x \in Z^+)$.
PROOF
2 is prime.
x^2 is the product of the two integers x and x.
2 divides x^2.
$\therefore$ 2 divides x or 2 divides x.
$\therefore$ 2 divides x.

Thus

2 divides $x^2 \Rightarrow$ 2 divides x.
$\therefore$ 2 does not divide $x \Rightarrow$ 2 does not divide x^2.

Q.E.D. ■

* For $a, b \in Z$, a is said to *divide* (be a *divisor* of) b if there exists $c \in Z$ such that $b = ac$. A *prime number* is an integer $p > 1$ such that the only divisors of p are ± 1, $\pm p$.

17.2.3 Methods of Direct Proof

17.2.3

Discussion * *

We have already defined a *direct proof* to be a chain of argument which leads directly from axioms and definitions (or hypotheses) to the theorem which we wish to prove (see page 34).

In this section and that which follows, we shall make no distinction between *proof* and *disproof*, since the negative aspect of the latter can always be expressed in the positive aspect of the former; that is, a *disproof* of proposition **a** is merely a *proof* of the proposition $\sim$**a** (or alternatively, a *proof* that **a** is FALSE).

Definition 1 * *

We look first at a method of proof which we have already used and which is known as proof by exhaustion (see *Unit 11*, *Logic I*). The method consists of examining every possible case; it is only practicable if we have a comparatively small number of possibilities. For example, in the solution of part (ii) of Exercise 17.2.2.1 we consider all four possible combinations of the truth values of **a** and **b**. We give one further example.

Example 1

Example 1

GIVEN The set $\{a, b, c, d\}$.

The binary operation $\circ$ on the set defined by:

$\circ$	a	b	c	d
a	a	c	d	b
b	c	b	a	d
c	d	a	c	a
d	b	d	a	d

(Remember that in such tables the combination $c \circ d$, say, is found as the element, a, in the intersection of the row beginning with c at the left end and the column beginning with d at the top.)

TO PROVE $\circ$ is commutative.

PROOF BY EXHAUSTION

From the table, we have (excluding $a \circ a$, $b \circ b$, etc.)

$$a \circ b = b \circ a$$

$$a \circ c = c \circ a$$

$$a \circ d = d \circ a$$

$$b \circ c = c \circ b$$

$$b \circ d = d \circ b$$

$$c \circ d = d \circ c$$

As we have exhausted all the possibilities we have proved that $\circ$ is commutative. Q.E.D. ■

Discussion * *

We are sometimes tempted to leap to a conclusion when we have not entirely exhausted all the possibilities, but have merely investigated what we consider to be a sufficiently large number of them. This sometimes gives rise to the fallacy of incomplete exhaustion. Of course, in some cases, an inadequately substantiated deduction turns out to be correct after all. We shall consider two simple examples.

Definition 2 *

(*continued on page 36*)

Solution 17.2.2.1

Solution 17.2.2.1

(i) Eggs are expensive.
Rule of detachment.

(ii) $\sim \mathbf{b} \Rightarrow \sim \mathbf{a}$
$\sim \mathbf{a} \vee \mathbf{b}$
$\sim(\mathbf{a} \wedge \sim \mathbf{b})$

a	b	~a	~b	~b ⇒ ~a	~a ∨ b	a ∧ ~b	~(a ∧ ~b)
0	0	1	1	1	1	0	1
0	1	1	0	1	1	0	1
1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	1

The columns in red are the same as that for $\mathbf{a} \Rightarrow \mathbf{b}$ (see page 31).

(iii) (hypothesis — arises from definition of a prime)
(hypothesis — arises from definition of x^2)
(taken as hypothesis — this is the opposite of what is to be proved)
(rule of detachment)
(rule of equivalence)
(summary of theorem so far)
(rule of equivalence) ■

(*continued from page 35*)

Example 2

Example 2

CONJECTURE $\forall_x 2^{2^x} + 1$ is a prime $(x \in Z^+)$.

This was once thought to be TRUE on the basis that:

$$2^{2^1} + 1 = 2^2 + 1 = 5 \text{ is a prime;}$$

$$2^{2^2} + 1 = 2^4 + 1 = 17 \text{ is a prime;}$$

$$2^{2^3} + 1 = 2^8 + 1 = 257 \text{ is a prime.}$$

This is a very slender exhaustive process, since only three cases are considered.* However, at first sight the conjecture seems plausible. Eventually it was shown that

$$2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297$$
$$= 641 \times 6\,700\,417$$

and so the conjecture was proved to be false. ■

Example 3

Example 3

CONJECTURE Every odd positive integer is equal to the sum of a prime number and twice the square of an integer.

If we start trying to prove this by considering specific examples, we obtain (neglecting the prime numbers, which can be expressed in the

* We have, in fact, presented a rather unfair picture of this conjecture, since more than three cases were thought to hold as the large numbers obtained had not been factorized.

form $x + 0^2$):

$9 = 7 + 2\cdot1^2$ (or $1 + 2\cdot2^2$)

$15 = 13 + 2\cdot1^2$ (or $7 + 2\cdot2^2$)

$21 = 19 + 2\cdot1^2$ (or $13 + 2\cdot2^2$ or $3 + 2\cdot3^2$)

$25 = 23 + 2\cdot1^2$ (or $17 + 2\cdot2^2$ or $7 + 2\cdot3^2$)

$27 = 19 + 2\cdot2^2$

$33 = 31 + 2\cdot1^2$ (or $1 + 2\cdot4^2$)

$35 = 17 + 2\cdot3^2$ (or $3 + 2\cdot4^2$)

. . . and so on.

In fact, we can continue a very long way (until we arrive at 5777) before we discover an odd number which does not have the property described. ■

Pierre Fermat

Discussion ★ ★

In each of the examples just quoted, we cannot expect to complete a proof by exhaustion that the conjecture is TRUE, since we are dealing with an infinite set of possibilities. Notice, however, that the case-by-case investigation of an infinite set of possibilities is useful if the conjecture is FALSE and at the same time universally quantified. In order to prove that a universally quantified conjecture is FALSE, we need only to find *one case* which does not hold. Such a case is called a counter-example, and, if a counter-example exists, an exhaustive case-by-case investigation (assuming this is possible) is bound to find it in the end, though it may take a very long time.

Definition 3 ★ ★ ★

Example 4

Example 4

CONJECTURE The proposition:

$$\exists_{x,y,z} x^n + y^n = z^n \qquad (x, y, z \in Z^+, n \in Z^+)$$

is TRUE only when $n = 1$ and $n = 2$.

This is called *Fermat's Last Theorem*, after PIERRE FERMAT, 1601–1665, who first put forward the conjecture in 1637. This conjecture has never been proved, and no counter-example has ever been found. ■

Example 5

Example 5

CONJECTURE No map on the page of an atlas requires more than four colours in order that no two countries with a common boundary shall be coloured the same.

This conjecture has never been proved, and no counter-example has ever been found. All map and atlas printers, however, accept it to be TRUE for practical purposes. ■

Discussion ★

Let us now consider why we were careful to specify that to prove a conjecture to be FALSE by a counter-example, the conjecture should be *universally quantified.*

If $\mathbf{a}_x$ is some open sentence with x as a variable, then we may quantify it in one of two ways. We may have either

$$\forall_x \mathbf{a}_x \qquad (x \in \text{some set } S)$$

or

$$\exists_x \mathbf{a}_x \qquad (x \in S).$$

If we have conjectured that $\mathbf{a}_x$ is TRUE for *all* $x \in S$, it requires only one counter-example to prove that this conjecture is FALSE.

This counter-example must, however, arise from an element of the specified set S. Suppose, however, that we have conjectured that $\mathbf{a}_x$ is TRUE for *some* $x \in S$. In this case, we must show that $\mathbf{a}_x$ is TRUE for *no* $x \in S$ in order to prove the conjecture FALSE, and, if S is an infinite set, we are back again with our problem of being unable to examine every case of an infinite set by the exhaustive method.

Example 6

Example 6

Consider the open sentence:

$$x^2 + 5 = 9.$$

(i) $\forall_x x^2 + 5 = 9 \qquad (x \in R).$

$x = 0$ is a counter-example, so the conjecture is proved FALSE.

(ii) $\exists_x x^2 + 5 = 9 \qquad (x \in R).$

This is proved TRUE by finding a single case, $x = 2$ (say).

(iii) $\forall_x x^2 + 5 = 9 \qquad (x \in \{-2, 2\}).$

This is proved TRUE by exhaustion, by investigating the 2 possible cases.

(iv) $\exists_x x^2 + 5 = 9 \qquad (x \in Z^+ \wedge x > 2).$

We know this to be FALSE, but in order to *prove* it so by exhaustion we would have to investigate an infinite number of cases: $x = 3$, $x = 4$, etc. We would therefore prove it FALSE by some other method.

(v) $\forall_x x^2 + 5 = 9 \qquad (x \in Z \wedge x^2 \in Z^-).$*

In this case the set to which x belongs is empty, so no counter-example exists to disprove the conjecture. Having therefore accepted it as TRUE, however, we cannot conclude that

$$\exists_x x^2 + 5 = 9 \qquad (x \in Z \wedge x^2 \in Z^-)$$

since no $x \in \varnothing$ exists. (See the discussion on page 28.) ■

Summary
* * *

We summarize our discussion about proof by exhaustion and counter-examples, as follows:

$\forall_x \mathbf{a}_x \qquad (x \in \text{some set } S)$:

may be proved TRUE by the method of exhaustion over S; may be proved FALSE by a counter-example from S.

$\exists_x \mathbf{a}_x \qquad (x \in S)$:

may be proved TRUE by an example from S; may be proved FALSE by the method of exhaustion over S.

Also, if

"$\forall_x \mathbf{a}_x \qquad (x \in S)$" is TRUE,

then

"$\exists_x \mathbf{a}_x \qquad (x \in S)$" is TRUE

provided that S is not empty.

Discussion
* *

We come now to the method of direct proof which has often been described as the peculiarly mathematical proof. This is the method of proof by *mathematical induction.* (Note that in the Introduction on page 2 we

* Z^- is the set of negative integers.

have already made the point that this is not to be confused with so-called inductive proof. See also *Polya**, page 114.)

The kind of conjecture to which proof by mathematical induction is applicable is a universally quantified open sentence for which the variable ranges over the set of positive integers, Z^+ (or, more generally, over any set that can be put in one–one correspondence with the positive integers); that is, a conjecture of the form:

$$\forall_n \mathbf{a}_n \qquad (n \in Z^+)$$

(or, for example, more generally:

$$\forall_n \mathbf{a}_n \qquad (n \in Z^+ \text{ and } n > r),$$

where r is a positive integer). In describing proof by mathematical induction, we shall assume initially that n ranges over the entire set Z^+.

The method consists of two parts:

(1) First, we *prove* that $\mathbf{a}_n$ is TRUE for $n = 1$;

(2) Secondly, we *prove* that if $\mathbf{a}_n$ is *assumed* to be TRUE for n equal to some arbitrary $k \in Z^+$, then it follows that $\mathbf{a}_n$ is TRUE also for $n = k + 1$.

Having proved (1) and (2) we then argue as follows:

since $\mathbf{a}_n$ is TRUE for $n = 1$,

it must also be TRUE for $n = 1 + 1 = 2$,

and for $n = 2 + 1 = 3$,

and for $n = 3 + 1 = 4$,

and so on,

hence $\mathbf{a}_n$ is TRUE for all $n \in Z^+$.

The basis of our argument is the *axiom of mathematical induction*, which we discuss on page 41 after giving three specific examples.

Example 7

Example 7

TO PROVE $\forall_n D^n(x \longmapsto xe^x) = x \longmapsto (x + n)e^x \qquad (n \in Z^+)$,

where D is the differentiation operator, and the functions both have domain R.

PROOF BY MATHEMATICAL INDUCTION

FIRST STEP

Consider the case $n = 1$.

$$\begin{aligned} D(x \longmapsto xe^x) &= x \longmapsto xe^x + e^x && \text{(product rule for differentiation)} \\ &= x \longmapsto (x + 1)e^x && \text{(distributivity)} \end{aligned}$$

SECOND STEP

Assume

$$\begin{aligned} D^k(x \longmapsto xe^x) &= x \longmapsto (x + k)e^x \ (k \in Z^+) && \text{(hypothesis)} \\ D^{k+1}(x \longmapsto xe^x) &= D[D^k(x \longmapsto xe^x)] && \text{(definition of differentiation operator)} \\ &= D[x \longmapsto (x + k)e^x] && \text{(hypothesis)} \\ &= x \longmapsto (x + k)e^x + e^x && \text{(product rule for differentiation)} \\ &= x \longmapsto [x + (k + 1)]e^x && \text{(distributivity and associativity).} \end{aligned}$$

* G. Polya, *How to Solve It*, Open University ed. (Doubleday Anchor Books 1970). This book is the set book for this course; it is referred to in the text as *Polya*.

Since the conjecture is proved to be TRUE for $n = 1$, and also for $n = k + 1$ whenever it is TRUE for $n = k$ $(k \in Z^+)$, it follows that it is TRUE for $n = 2, 3, 4, \ldots$ and so for all $n \in Z^+$. The conjecture is therefore proved by mathematical induction to be TRUE, and can be accepted as a *theorem* of the calculus. (Notice, however, that we have had to accept another theorem and certain properties and definitions during the proof.) ■

Example 8

Example 8

GIVEN $u_1 = 1$

$u_2 = 2$

$\forall_n u_n = u_{n-1} + u_{n-2}$ $\quad (n \in Z^+ \text{ and } n > 2)$

TO PROVE $\forall_n u_n < (7/4)^n$ $\quad (n \in Z^+)$.

In this case, the recurrence formula is defined for $n > 2$ only, so we first note that

$$u_1 = 1 < (7/4)^1$$

and

$$u_2 = 2 < (7/4)^2.$$

Then we use the method of mathematical induction: the first step is to prove the proposition true for $n = 3$, and then we continue as before, except that k now belongs to the set of positive integers greater than 2.

PROOF BY MATHEMATICAL INDUCTION

FIRST STEP

Consider the case $n = 3$.

$$\begin{aligned} u_3 &= u_2 + u_1 && \text{(given)} \\ &= 2 + 1 && \text{(given)} \\ &= 3 \\ &< (7/4)^3 \end{aligned}$$

SECOND STEP

Assume

$$\begin{aligned} u_k &< (7/4)^k \ (k \in \{3, 4, 5, \ldots, n-1\}) && \text{(hypothesis)} \\ u_n &= u_{n-1} + u_{n-2} && \text{(given)} \\ &< (7/4)^{n-1} + (7/4)^{n-2} && \text{(hypothesis and property of inequality)} \\ &= (7/4)^{n-2}(1 + 7/4) \end{aligned}$$

Now

$$(1 + 7/4) = 11/4 < (7/4)^2$$

so

$$\begin{aligned} u_n &< (7/4)^{n-2}(7/4)^2 && \text{(property of inequality)} \\ &= (7/4)^n. \end{aligned}$$

We can now infer that the conjecture is TRUE for $n = 3, 4, 5, \ldots$, and we have already noted that it is TRUE for the cases $n = 1$ and $n = 2$.

So the conjecture has been proved to be TRUE and can be accepted as a *theorem*. ■

Example 9

Example 9

TO PROVE The sum, S_n, of the interior angles of a convex polygon of n sides is $180(n-2)°$.

PROOF BY MATHEMATICAL INDUCTION

FIRST STEP

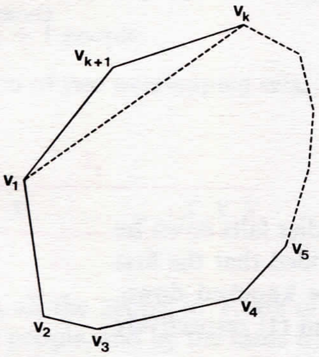
Consider the case $n = 3$.

$$180(3-2)° = 180°,$$

which is the sum of the interior angles of a triangle (a theorem of Euclidean geometry); so $180(3-2)° = S_3$.

SECOND STEP

Consider a convex polygon of $k + 1$ sides, as shown:



If we connect vertex v_1 to vertex v_k (as shown) then the polygon is divided into a triangle and a convex polygon of k sides.

Assume

$$S_k = 180(k-2)° \qquad (k \in Z^+ \text{ and } k > 2).$$

$$\begin{aligned} S_{k+1} &= S_k + S_3 \\ &= S_k + 180° \\ &= 180(k-2)° + 180° \\ &= 180(k-1)° \\ &= 180[(k+1)-2]°. \end{aligned}$$

The proof can now be completed, as the two steps have been proved.

(Notice that here again we have assumed certain theorems; for example, the sum of the interior angles of a triangle, and properties of chords of convex polygons, etc.) ■

Discussion
* *

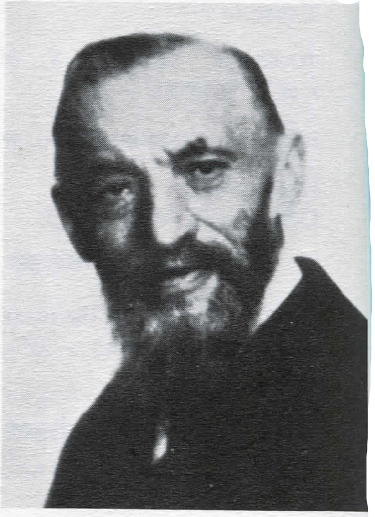
It is important to note that the whole basis of proof by mathematical induction depends upon certain properties of the positive integers. In particular, we need to have a criterion for deciding whether a given set S of positive integers includes *all* the positive integers. We fall back upon what is called the axiom of mathematical induction:

Axiom of Mathematical Induction
* * *

Given that S is a subset of Z^+, if

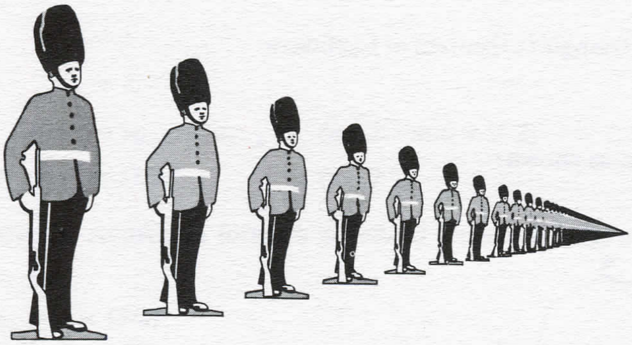
(1) the integer $1 \in S$
and
(2) the integer $k + 1 \in S$ whenever $k \in S$,
then $S = Z^+$.

This axiom was first framed by GUISEPPE PEANO, 1858–1932, and is equivalent to a set of postulates known as Peano's postulates.



Guiseppe Peano

We can understand this axiom intuitively by thinking of an endless straight single file of tin soldiers, beginning at some point and then continuing for ever.



Provided that the soldiers are so spaced that if any soldier falls down he automatically knocks down the next soldier, and provided that the first soldier is knocked down, then all the soldiers will be knocked down. These two conditions correspond to conditions (2) and (1) respectively of the axiom.

The relation of the axiom of mathematical induction to proof by mathematical induction can be seen as follows:

Let S be the subset of Z^+ containing all the positive integers n for which a conjecture $\mathbf{a}_n$ is true.

Then S is given as required by the axiom. The first step of a proof by mathematical induction shows that (1) of the axiom holds. The second step of a proof shows that (2) of the axiom holds.

The axiom now tells us that $S = Z^+$, thus proving $\mathbf{a}_n$ as a theorem.

Exercise 1

Exercise 1

(i) Determine whether the binary operation of Example 1 (page 35) is (3 minutes)

(a) closed;
(b) associative.

What kind of proof did you use in each case?

(ii) Given that (2 minutes)

$$\exists_x \mathbf{a}_x \qquad (x \in S)$$

is FALSE, may we deduce that

$$\forall_x \mathbf{a}_x \qquad (x \in S)$$

is FALSE? Give reasons for your answer.

(iii) Prove by mathematical induction that: (10 minutes)

(a) $\forall_n n! > 2^n \qquad (n \in Z^+ \text{ and } n > 3)$

(HINT: Having made your assumption about $k!$ consider $5 \times (k!)$);

(b) n independent propositions can be assigned truth values in 2^n distinct ways ($n \in Z^+$).

(iv) Prove that if (3 minutes)

$$2 + 4 + 6 + \cdots + 2n = n^2 + n + 1 \qquad (n \in Z^+)$$

is TRUE for $n = k$, then it is TRUE for $n = k + 1$. Why cannot you complete the proof by mathematical induction that it is true for all $n \in Z^+$?

(v) What is wrong with the following "proof"? (5 minutes)

CONJECTURE

$\forall_n$ If S is a set of n people, then all are of the same sex ($n \in Z^+$).

PROOF BY MATHEMATICAL INDUCTION

FIRST STEP

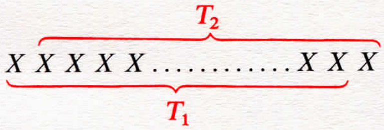
Consider the case $n = 1$; the proposition is obviously true in this case.

SECOND STEP

Assume the proposition true for $n = k$ ($k \in Z^+$).

Let T be a set of $k + 1$ people.

Then T is the union of two overlapping sets, T_1, T_2, each containing k people.



By the hypothesis, all the people in T_1 are of the same sex, since T_1 contains exactly k people, and by the same hypothesis all the people in T_2 are of the same sex for the same reason. But T_1 and T_2 overlap. Hence, all the people in T are of the same sex. So if the conjecture is TRUE for $n = k$, it is TRUE for $n = k + 1$. It has been proved TRUE for $n = 1$, hence it is TRUE for $n = 1, 2, 3, \ldots$ and hence for all $n \in Z^+$.

■

Discussion
★★

In the course of your studies of mathematics you may have come across the expression *necessary and sufficient conditions.* The concept plays a very important part in mathematical proof, and so we are going to investigate it here. Before doing so, however, we need to consider the relation between certain special kinds of proposition.

Consider some *valid* statement of the form

a ⇒ **b**.

An example of this is:

All equiangular triangles are isosceles,

since this can be put in the equivalent form:

If a triangle is equiangular, *then* it is isosceles.

Definition 4
★★★

The converse of **a** ⇒ **b** is obtained by interchanging **a** and **b** to give

b ⇒ **a**,

which, translated into our triangle example, would be equivalent to:

All isosceles triangles are equiangular,

or

If a triangle is isosceles, then it is equiangular.

Now it is quite obvious from the example which we have chosen, that the converse of a proposition does not follow from the proposition

(*continued on page 45*)

Solution 1

(i) (a) YES. We see that in every case we obtain an element of the original set. Proof by exhaustion.

(b) NO. For example

$$(a \circ b) \circ c = c \circ c = c$$

but

$$a \circ (b \circ c) = a \circ a = a$$

Conjecture FALSE by counter-example.

(ii) NO. The set S may be empty, in which case

$$\exists_x \mathbf{a}_x \quad (x \in S) \quad \text{is} \quad \text{FALSE, yet}$$

$$\forall_x \mathbf{a}_x \quad (x \in S) \quad \text{is} \quad \text{TRUE.}$$

(iii) (a) FIRST STEP Consider the case $n = 4$:

$$\left.\begin{aligned} 4! &= 4 \times 3 \times 2 \times 1 = 24 \\ 2^4 &= 16 \end{aligned}\right\} \text{so } 4! > 2^4$$

SECOND STEP

Assume $k! > 2^k$ ($k \in Z^+$ and $k > 3$); then

$$5 \times k! > 5 \times 2^k \cdots (A)$$

Now $k + 1 \geqslant 5$, so

$$(k + 1) \times k! \geqslant 5 \times k! \cdots (B)$$

From (A) and (B),

$$(k + 1) \times k! > 5 \times 2^k > 2 \times 2^k$$

i.e.

$$(k + 1)! > 2^{k+1}.$$

If the conjecture is TRUE for k ($k \in Z^+$ and $k > 3$), then it is TRUE for $k + 1$. It is TRUE for $k = 4$, hence for $k = 5, 6, 7, \ldots$, that is, for all positive integers greater than 3.

(Various assumptions are made about properties of factorial powers of numbers, inequalities, etc.)

(b) FIRST STEP Consider the case $n = 1$; the conjecture is clearly true, since one given proposition can be assigned one only of the two truth values corresponding to TRUE, FALSE.

SECOND STEP

Assume the conjecture is TRUE for $n = k$ ($k \in Z^+$).

Now $k + 1$ propositions can be assigned truth values in 2×2^k ways, since we have assumed that k propositions can be assigned truth values in 2^k ways, and to each of these ways there corresponds the $(k + 1)$th proposition being TRUE and the same proposition being FALSE. Since $2 \times 2^k = 2^{k+1}$, the second step is proved, and the proof by mathematical induction can be completed.

(iv) PROOF

Assume

$$2 + 4 + 6 + \cdots + 2k = k^2 + k + 1;$$

then

$$\begin{aligned} 2 + 4 + 6 + \cdots + 2k + 2(k + 1) &= k^2 + k + 1 + 2(k + 1) \\ &= k^2 + 2k + 1 + k + 1 + 1 \\ &= (k + 1)^2 + (k + 1) + 1. \end{aligned}$$

Hence the conjecture is TRUE for $n = k + 1$. The conjecture is FALSE for $n = 1$, since

$$2 \neq 1^2 + 1 + 1 = 3.$$

In fact, the conjecture is TRUE for *no* n ($n \in Z^+$), and this underlines the necessity for the first step as well as the second in a proof by mathematical induction.

(v) The proof fails in going from $n = 1$ to $n = 2$; that is the second step is not valid for the case:

$$\underbrace{X}_{T_1}\ \overbrace{X}^{T_2}$$

The intersection of T_1 and T_2 is empty, and so argument from "overlap" completely fails. ■

(*continued from page 43*)

itself. This leads us to state a very important (if apparently obvious) principle in logic, namely:

> The truth of a conclusion does not imply the truth of the hypotheses from which the conclusion was deduced.

To emphasize this, we give another very simple example:

Example 10

Example 10

HYPOTHESIS

$$x = y \qquad (x, y \in Z^+).$$

DEDUCTION

If $x = y$, then $y = x$.

$\therefore$ By the theorem on dividing equals by equals, we have:

$$\frac{x}{x} = \frac{y}{y}$$

whence

$$1 = 1.$$

"The conclusion is manifestly TRUE, so the hypothesis is TRUE, therefore all positive integers are equal." This is manifestly nonsense, and the fallacy lies in the step which purports to deduce the hypothesis from the admittedly TRUE conclusion.

(Although so obviously fallacious when presented in this form, every teacher of mathematics is aware how often this form of invalid reasoning is used to "prove" a result given in the statement of the problem.) ■

Discussion
* *

In contrast to the situation we have with the converse, suppose again that we have a *valid* statement of the form

$$\mathbf{a} \Rightarrow \mathbf{b}.$$

What happens if, we can prove that **b** is FALSE? Reference to our truth table for $\mathbf{a} \Rightarrow \mathbf{b}$ shows us that if $\mathbf{a} \Rightarrow \mathbf{b}$ is TRUE and **b** is FALSE, then **a** is FALSE.

a	b	$\mathbf{a} \Rightarrow \mathbf{b}$
0	0	1
0	1	1
1	0	0
1	1	1

(Since **b** is FALSE, we need only look at rows 1 and 3. But we said that $\mathbf{a} \Rightarrow \mathbf{b}$ is TRUE. This disqualifies the third row, since there is a 0 under $\mathbf{a} \Rightarrow \mathbf{b}$, and in the top row we have a zero under **a**, so we see that **a** is FALSE.)

So, we have another important principle, namely:

> The falsehood of a conclusion of a valid argument implies the falsehood of a hypothesis.

(We say "a" hypothesis here, since our argument may be based on several hypotheses, only one of which may be FALSE.)

What we have said, in effect, is that from

$$\mathbf{a} \Rightarrow \mathbf{b}$$

we can deduce that

$$\sim\mathbf{b} \Rightarrow \sim\mathbf{a},$$

a result which we could also have deduced by writing out the truth table for the latter proposition.

Definition 5
* *

The proposition $\sim\mathbf{b} \Rightarrow \sim\mathbf{a}$ is called the contrapositive of $\mathbf{a} \Rightarrow \mathbf{b}$. It should be carefully contrasted with the *converse* of $\mathbf{a} \Rightarrow \mathbf{b}$, which is $\mathbf{b} \Rightarrow \mathbf{a}$.

We return now to the concept of *necessary and sufficient conditions*.

The proposition

$$\mathbf{a} \Rightarrow \mathbf{b}$$

Definition 6
* * *

means that **a** is a sufficient condition for **b**. The truth of **a** is *sufficient* to ensure the truth of **b**.

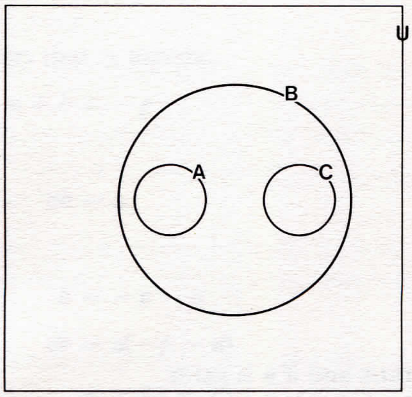
The converse proposition

$$\mathbf{b} \Rightarrow \mathbf{a}$$

Definition 7
* * *

means that **a** is a necessary condition for **b**. If **b** is TRUE, then it *necessarily* follows that **a** is TRUE.

To understand just what all this is about, consider the following Venn diagram, in which $A \cap C$ is shown empty:



Let **a**, **b**, **c** represent the propositions

$$x \in A, \qquad x \in B, \qquad x \in C$$

respectively, for some element x of U. Notice that we have as TRUE propositions:

$$\mathbf{a} \Rightarrow \mathbf{b}$$

and

$$\mathbf{c} \Rightarrow \mathbf{b}.$$

Also, we have as a FALSE proposition

$$\mathbf{a} \wedge \mathbf{c}.$$

We see that **a** is not the only proposition implying **b**, so that although **a** is *sufficient* for **b**, there may well be other propositions such as **c** *sufficient* for **b**. Further, such propositions **c** may be TRUE only when **a** is FALSE. It is thus *not necessary* for **a** to be TRUE in order that **b** be TRUE. On the other hand, unless **b** is TRUE, neither **a** nor **c** can be TRUE, so **b** is a *necessary* condition for **a** and also a *necessary* condition for **c**, even though $\mathbf{a} \wedge \mathbf{c}$ is never TRUE. So the truth of **b** is *not sufficient* to *guarantee* either the truth of **a** or the truth of **c**.

It is not difficult to see that for propositions **a** and **b** (above), if **a** is to be a *necessary AND sufficient* condition for **b**, then we require that

$$\mathbf{a} \Rightarrow \mathbf{b}$$

and

$$\mathbf{b} \Rightarrow \mathbf{a},$$

that is,

$$A = B.$$

From section 11.1.4, *Unit 11*, *Logic I*, we know that

$$(\mathbf{a} \Rightarrow \mathbf{b}) \wedge (\mathbf{b} \Rightarrow \mathbf{a})$$

is equivalent to

$$\mathbf{a} \Leftrightarrow \mathbf{b},$$

and from the truth table for $\mathbf{a} \Leftrightarrow \mathbf{b}$, namely:

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{a} \Leftrightarrow \mathbf{b}$
0	0	1
0	1	0
1	0	0
1	1	1

we see that $\mathbf{a} \Leftrightarrow \mathbf{b}$ means that if **a** is TRUE then **b** is TRUE and if **a** is FALSE then **b** is FALSE. We also know from section 11.1.7, *Unit 11*, that $\Leftrightarrow$ is *self-transitive*:

$$[(\mathbf{a} \Leftrightarrow \mathbf{b}) \Leftrightarrow (\mathbf{b} \Leftrightarrow \mathbf{c})] \Leftrightarrow (\mathbf{a} \Leftrightarrow \mathbf{c}).$$

So there are several ways of proving necessary and sufficient conditions. We may prove:

$$(\mathbf{a} \Rightarrow \mathbf{b}) \wedge (\mathbf{b} \Rightarrow \mathbf{a}),$$

or we may prove:

$$(\mathbf{a} \Rightarrow \mathbf{b}) \wedge (\sim\mathbf{a} \Rightarrow \sim\mathbf{b}),$$

or we may prove:

$$\mathbf{a} \Leftrightarrow \mathbf{b}_1 \Leftrightarrow \mathbf{b}_2 \Leftrightarrow \cdots \Leftrightarrow \mathbf{b}.$$

The proposition

$$\sim\mathbf{a} \Rightarrow \sim\mathbf{b}$$

Definition 8
* *

is known as the inverse of $\mathbf{a} \Rightarrow \mathbf{b}$, and so proving necessary and sufficient conditions involves either the proof of a *proposition and its converse*, or the proof of a *proposition and its inverse*, or it may involve what is known as an *iff-string*, since $\mathbf{a} \Leftrightarrow \mathbf{b}$ can be read as "**a** if and only if **b**" (abbreviated to "**a** iff **b**").

Example 11 **Example 11**

TO PROVE

$$\left.\begin{aligned} a + b &= -p \\ ab &= q \end{aligned}\right\} \qquad (a, b \in R)$$

are necessary and sufficient conditions for a, b to be the roots of the equation

$$x^2 + px + q = 0 \qquad \text{where } p^2 > 4q.$$

PROOF

Let **a** represent

$$a + b = -p \quad \text{and} \quad ab = q \qquad (a, b \in R),$$

and **b** represent

$$a, b \text{ are roots of the equation } x^2 + px + q = 0.$$

We need to show

$$\mathbf{a} \Rightarrow \mathbf{b} \qquad \text{(sufficiency)}$$

and

b ⇒ **a** (necessity).

SUFFICIENCY

Assume that **a** is true; that is, assume

$$a + b = -p$$

and

$$ab = q.$$

Then,

$$b = -p - a$$

$$\therefore \quad ab = a(-p - a)$$

$$= -pa - a^2.$$

Also

$$ab = q$$

$\therefore \quad a^2 + pa + q = 0$

$\therefore \quad a$ is a root of the given equation.

Similarly,

b is a root of the given equation.

Thus

b is true whenever **a** is true, that is, **a** ⇒ **b**.

NECESSITY

Assume that **b** is true; that is, assume a, b to be roots of the given equation. By the formula for the roots of a quadratic, we have (say)

$$a = \frac{-p + \sqrt{p^2 - 4q}}{2}$$

(See RB5)

$$b = \frac{-p - \sqrt{p^2 - 4q}}{2}$$

$\therefore \quad a + b = -p$

and

$$ab = \frac{(-p)^2 - (p^2 - 4q)}{4} = q.$$

Thus **a** is true whenever **b** is true, that is, **b** ⇒ **a**. So **a** ⇒ **b** and **b** ⇒ **a**, and the proof is complete. ■

Exercise 2

Exercise 2
(4 minutes)

(i) Given the following propositions as hypotheses:

$$\mathbf{a} \Rightarrow \mathbf{b} \qquad (1)$$

$$\mathbf{b} \Rightarrow \mathbf{a} \qquad (2)$$

$$\sim\mathbf{a} \Rightarrow \sim\mathbf{b} \qquad (3)$$

$$\sim\mathbf{b} \Rightarrow \sim\mathbf{a} \qquad (4)$$

indicate which of the following are TRUE and which are FALSE:

(a) $(1) \Rightarrow (2)$

(b) $(1) \Rightarrow (3)$

(c) $(1) \Rightarrow (4)$

(d) $(2) \Rightarrow (3)$

(e) $(2) \Rightarrow (4)$

(f) $(3) \Rightarrow \sim(1)$

(g) $\sim(3) \Rightarrow \sim(4)$

(h) $(4) \Rightarrow (1)$

(ii) Prove that a necessary and sufficient condition for an integer to be *even* is that *its square is even*, by proving a proposition and
(a) its *converse*;
(b) its *inverse*. ■

(5 minutes)

17.2.4 Methods of Indirect Proof

17.2.4

Discussion
**

We have defined *indirect proof* as a proof of a proposition equivalent to that which we want to prove, and we pointed out that in general the *rule of substitution* allows us to turn an *indirect proof* into a *direct proof* by adding one further step.

However, there is one particular method of indirect proof, in which we prove that $\sim\mathbf{a}$ is FALSE when we want to prove that $\mathbf{a}$ is TRUE, and we prove $\sim\mathbf{a}$ is FALSE by assuming that it is TRUE and showing that this leads to a contradiction. Such a proof is called proof by contradiction (or *reductio ad absurdum*).*

Definition 1
***

This method of proof is used very frequently in mathematics, and there are a number of theorems for which no other method of proof has been discovered.

Let us look at an example of a proof by contradiction. (The one we have selected is probably the first such proof ever to be completed.)

Example 1

Example 1

TO PROVE

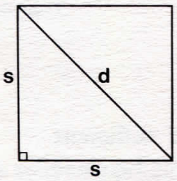
For a square, the ratio: $\dfrac{\text{length of side}}{\text{length of diagonal}}$ cannot be expressed as $\dfrac{x}{y}$, where $x, y \in Z^{+}$ and have no common divisor.

PROOF BY CONTRADICTION

Let s be the length of a side and let d be the length of a diagonal. Then assume as a hypothesis the contradiction of the conjecture; that is, if the hypothesis is $\mathbf{a}$, we assume that $\sim\mathbf{a}$ is TRUE, that is:

$$\frac{s}{d} = \frac{x}{y} \qquad \text{(where } x \text{ and } y \text{ have no common divisor)}$$

$$\therefore \quad \frac{s^2}{d^2} = \frac{x^2}{y^2}.$$



By Pythagoras' theorem, $d^2 = 2s^2$, so

$$\frac{s^2}{d^2} = \frac{s^2}{2s^2} = \tfrac{1}{2}.$$

But

$$\frac{s^2}{d^2} = \frac{x^2}{y^2}$$

$$\therefore \quad \frac{x^2}{y^2} = \tfrac{1}{2}.$$

Now

$$y^2 = 2x^2 \Rightarrow y^2 \text{ is even} \Rightarrow y \text{ is even}$$

(since the square of an odd number is odd),
and x is odd,

[*] See also *Polya*, page 162.

(*continued on page 52*)

Solution 17.2.3.2

(i) (a) FALSE
(b) FALSE
(c) TRUE
(d) TRUE
(e) FALSE
(f) FALSE
(g) FALSE
(h) TRUE.

(ii) (a) Suppose x is *even* $(x \in Z)$.
Then

$$x = 2k \qquad \text{(for some } k \in Z\text{)},$$

so

$$x^2 = 4k^2$$
$$= 2(2k^2)$$

which is *even*. (necessity)

Now suppose x^2 is *even* $(x \in Z)$. Since x^2 is also a perfect square, it follows that $x^2 = 4k^2$ (for some $k \in Z^+$)

$$\therefore \quad x = \pm 2k$$

which is *even*. (sufficiency — converse)

(b) Suppose x is *not even* $(x \in Z)$. Then

$$x \text{ is } odd,$$

so

$$x = 2k + 1 \qquad \text{(for some } k \in Z\text{)}$$

and

$$x^2 = (2k + 1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

which is *odd*,

and therefore is *not even*. (sufficiency — inverse)

(Note that in this question we referred to "a" necessary and sufficient condition, not "the" necessary and sufficient condition. This is because such conditions are *not unique*. For example, if $\mathbf{b}_1 \Leftrightarrow \mathbf{b}_2 \Leftrightarrow \mathbf{b}_3 \Leftrightarrow \mathbf{a}$ then $\mathbf{b}_1, \mathbf{b}_2$ and $\mathbf{b}_3$ are all necessary and sufficient conditions for $\mathbf{a}$.) ■

(continued from page 51)

since x, y have no common divisor. Further, if y is even, then

$$y = 2z \text{ for some integer } z.$$

$$\therefore \quad y^2 = 4z^2.$$

But

$$y^2 = 2x^2,$$

$$\therefore \quad 2x^2 = 4z^2,$$

and

$$x^2 = 2z^2 \Rightarrow x^2 \text{ is even} \Rightarrow x \text{ is even}.$$

We have thus proved that x is odd and also that x is even, which is a contradiction.

Since the conclusion is contradictory and the reasoning valid, the hypothesis $\sim\mathbf{a}$ must be FALSE. If the hypothesis is FALSE, the original conjecture **a** must be TRUE.

(Note that this is in effect a proof that $\sqrt{2}$ is irrational; that is, it cannot be expressed as a ratio of two integers.) ■

Proof by contradiction and indirect proof by *proving a contrapositive* (see page 46) have something in common, but must not be confused with each other. In both cases we may set out to prove a conjecture having the form

$$\mathbf{a} \Rightarrow \mathbf{b}.$$

When we prove the *contrapositive* of this, namely

$$\sim\mathbf{b} \Rightarrow \sim\mathbf{a}$$

(which is an equivalent conjecture), we assume $\sim\mathbf{b}$ and from $\sim\mathbf{b}$ we deduce $\sim\mathbf{a}$.

To prove

$$\mathbf{a} \Rightarrow \mathbf{b}$$

by *contradiction*, we assume *both* **a** and $\sim\mathbf{b}$ and try to deduce either any proposition **c** and also its negation $\sim\mathbf{c}$, or some proposition **c** which contradicts a known theorem in the system in which we are working (or indeed one of our hypotheses **a** and $\sim\mathbf{b}$).

The similarity between the two methods lies only in the initial assumption of $\sim\mathbf{b}$.

We shall not discuss any further methods of indirect proof here; as we have seen, the rule of equivalence converts these into direct proofs except in the particular case of proof by contradiction (where there is the special reliance upon the *axiom of excluded middle*). Indirect proofs of one sort or another are used frequently in mathematics, particularly in the proofs of *existence theorems* (which assert that, e.g., the solution of an equation *exists*) and in the proofs of *uniqueness theorems* (which assert that, e.g., a solution of an equation is *unique*).

Exercise 1 **Exercise 1**

(i) Prove by contradiction: (3 minutes)

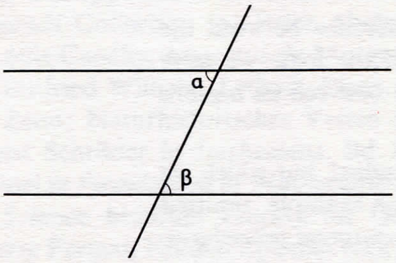
$$x \text{ is odd} \Rightarrow x^2 \text{ is odd} \qquad (x \in Z).$$

(ii) Prove the contrapositive of (2 minutes)

$$\forall_\varepsilon |x| < \varepsilon \Rightarrow x = 0 \qquad (\varepsilon \in R^+),$$

where x is a real number.

(iii) Prove that, in Euclidean geometry, if a straight line cuts two other straight lines in a plane so that the alternate angles are equal, then the two cut straight lines do not intersect. (3 minutes)



(HINT: Prove this by contradiction and use the theorem that the sum of the interior angles of a triangle is 180°.) ■

Solution 1

Solution 1

(i) Assume x is odd *and* x^2 is even $(x \in Z)$.

If x is odd, then

$$\begin{aligned} x &= 2k + 1 \qquad (k \in Z) \\ x^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

which is odd. But x^2 is even by hypothesis. Hence the hypothesis is FALSE and the given conjecture is TRUE.

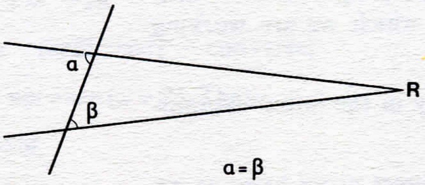
(ii) Assume $x \neq 0$.

This implies $|x| > 0$

$$\therefore \quad \exists_\varepsilon x \geqslant \varepsilon \qquad (\varepsilon > 0).$$

(For example, $\varepsilon = |x|$.)

(iii) Assume that the cut lines intersect at R. Let the acute angle between the lines at R be γ.



Then we have a triangle, the sum of whose interior angles is

$$\begin{aligned} &\gamma + \beta + (180 - \alpha) \\ &= \gamma + \beta + (180 - \beta) \\ &= \gamma + 180. \end{aligned}$$

But the sum of the interor angles of every triangle is 180°. This is a contradiction, since $\gamma > 0$. ■

17.2.5 Conclusion

17.2.5

Conclusion

* *

In section 17.2 we have surveyed proof in mathematics. We have not by any means exhausted the topic, and our examples have of necessity been selected from areas with which we assume you are familiar. Several of the examples deal with the properties of the positive integers, the integers, or the real numbers. In *Unit 34, Number Systems,* we shall be taking a closer look at numbers, beginning by accepting the natural numbers as primitive terms.

You will probably have noticed a considerable difference between the kind of logic which we considered in *Unit 11*, and the logic we have studied here. Broadly speaking, the difference is that between an *algebra of logic* and an *axiomatic theory of algebra.*

There are many other topics which we could have studied, but which we decided to leave for another occasion. We have, for example, omitted any discussion of *decision procedures*, and also of *computation procedures*, for both of which the word *algorithm* is often used. The question of whether something is *decidable* and the question of whether something is *computable* are important and distinct questions worthy of future study.

We shall end by once more referring to the distinction between *truth* and *validity*. In mathematics, we often use the word *truth* to mean *truth for the purposes of the particular problem.* Thus we may use it in the sense that

if $x = y$ is TRUE $\quad (x, y \in R)$
then it follows that
$2x = 2y$ is also TRUE.

If we go right back to the most primitive definition of number that we can invent, we shall find that, despite what we might think when we are actually calculating with numbers in a perfectly abstract manner, our roots are somehow or other embedded in the real world which surrounds us. In the last resort, the number x is only an abstraction from a great many sets, each of x things, such as

a set of two pigs;
a set of two children;
a set of two stars;

and so on.

We have seen that in any axiomatic theory we must start somewhere with *assumed* definitions and axioms. If these are not TRUE, then our reasoning may be *valid*, but we shall have no means of determining whether or not our conclusions are TRUE. Behind our basic assumption of what we accept initially as TRUE, there lie only *intuition* and *experience*. It is a good thing for every mathematician (and logician) to pause once in a while in his headlong pursuit of "truth", and to remember that, however beautiful and however massive the structure he has discovered or created, an occasional visit to the cellars to ensure that the foundations are secure is well worth while. Logic and mathematics may at first sight seem not only very abstract disciplines, but they may also seem very *sure* disciplines in that, provided we can find a way of correctly calculating or proving something, we are in a position to be pretty confident about the result.

If everything were absolutely cut-and-dried, then life would be pretty dull, so perhaps it is, after all, a good thing that there are still uncertainties at the foundations of mathematics, just as there are vast unexplored territories to be discovered. In whichever direction we pursue our studies there will always be, it seems, unsolved problems and unanswerable questions. One of the latter would appear to be:

Is there such a thing as an absolutely and certainly true proposition?

and that would seem to be more in the province of theology than logic or mathematics.

Acknowledgements

Grateful acknowledgement is made to the following sources for illustrations used in this correspondence text:

Dalloglio, Milan for Guiseppe Peano in *Storia della Scienzia*, Vol. 5, 1969, U. Forti; The Mansell Collection for Peter Abelard, Aristotle, Roger Bacon, Augustin Louis Cauchy, Augustus de Morgan, Charles Dodgson, Leonhard Euler, Gottfried Wilhelm Leibniz, Plato, Bernhard Riemann, Bertrand Russell, Zeno; Naturhistorisches Verein der Rheinlande and Westfalens for Ernst Schröder in *Decheniana*, Bd 122, 1969; Springer-Verlag for Kurt Gödel in *Foundations of Mathematics* by Buloff, Holyeake and Haln, 1969; Science Museum Library for George Boole, Georg Cantor, Euclid, Pierre Fermat, Nikolai Lobachevski, Pythagoras; Science Museum, London for John Venn, Alfred North Whitehead; Verlag Chemie for Raimon Lull in *Das Buch der Grossen Chemiker* Bd 1, 1929, G. Bugge.

Unit No.		Title of Text
1		Functions
2		Errors and Accuracy
3		Operations and Morphisms
4		Finite Differences
5	NO TEXT	
6		Inequalities
7		Sequences and Limits I
8		Computing I
9		Integration I
10	NO TEXT	
11		Logic I — Boolean Algebra
12		Differentiation I
13		Integration II
14		Sequences and Limits II
15		Differentiation II
16		Probability and Statistics I
17		Logic II — Proof
18		Probability and Statistics II
19		Relations
20		Computing II
21		Probability and Statistics III
22		Linear Algebra I
23		Linear Algebra II
24		Differential Equations I
25	NO TEXT	
26		Linear Algebra III
27		Complex Numbers I
28		Linear Algebra IV
29		Complex Numbers II
30		Groups I
31		Differential Equations II
32	NO TEXT	
33		Groups II
34		Number Systems
35		Topology
36		Mathematical Structures

SBN 335 01016 4